16 STRON EKSTRA

BEZPIECZNI KI VPN

PRAKTYCZNE TRIKI OD PODSTAW

PARTNER WYDANIA:
Surfshark®

Komputer Świat

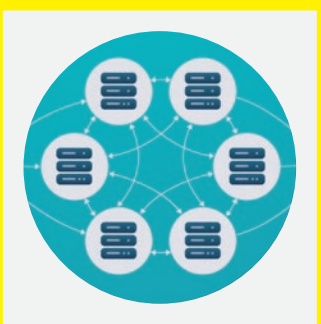
BEZPIECZNIE W SIECI DZIĘKI VPN

PRAKTYCZNE TRIKI OD PODSTAW

- **Nexus:** przełomowe zabezpieczenie połączeń
- Jakie dane **zbierają popularne aplikacje**
- **Co nam grozi** w razie wycieku danych

TO WARTO WIEDZIEĆ

W jaki sposób VPN **podnosi poziom bezpieczeństwa**



Jak skonfigurować VPN w Windows i na smartfonie

Jak monitorować naruszenia danych kart i kont e-mail

Dodatkowe funkcje **chroniące naszą prywatność**

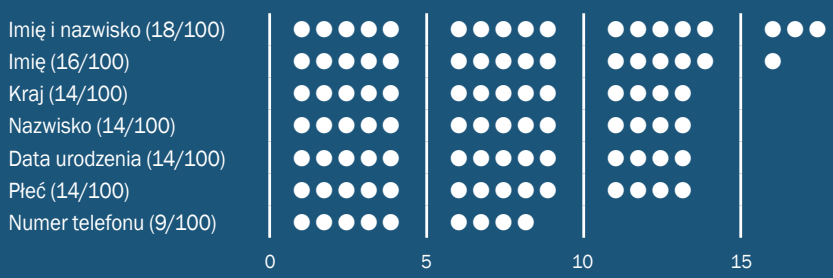
DLACZEGO ZACHOWANIE PRYWATNOŚCI W SIECI JEST WAŻNE

Na co dzień coraz częściej zdarza się, że jesteśmy w sieci przez całą dobę. Nasze smartfony bez przerwy są aktywne i otrzymujemy powiadomienia z mediów społecznościowych. Na komputerze również bez przerwy przeglądamy zasoby internetu. ***Warto zastanowić się, jakie dane i ślady po sobie zostawiamy i czy jest to bezpieczne***

Internet oferuje bardzo wiele możliwości. Pozwala szybko nawiązać kontakt z milionami innych użytkowników przez sieci społecznościowe, możemy dokonywać zakupów i udostępniać różnego rodzaju treści. Warto jednak zastanowić się, co się dzieje z naszą prywatnością, gdy na przykład wrzucamy do sieci zdjęcie informujące wszystkich, że jesteśmy na wakacjach. Gdy udostępniamy je publicznie, wszyscy wiedzą, gdzie jesteśmy w danej chwili. Ze względów bezpieczeństwa jest to problem. Z jednej strony wiadomo wtedy, gdzie nas nie ma, co może ułatwić dokonanie włamania. Z drugiej wiadomo też, gdzie jesteśmy i co robimy, co również może pomóc w kradzieży i pozwala wnioskować o naszym stanie posiadania.

DANE, KTÓRE NAJCZĘŚCIEJ WYCIEKAJĄ

Poniższe zestawienie pokazuje orientacyjnie, ile jakich rodzajów danych na 100 użytkowników ulega wyciekom. Im więcej informacji związanych z daną osobą znajdzie się w wycieku, tym łatwiej jest oszustom podszyć się pod nią lub oszukać osoby z jej otoczenia.



Prywatność a internet

Warto pamiętać, że zwykłe przeglądanie internetu niesie ze sobą szereg konsekwencji. Gdy odwiedzamy różne strony czy przechodzimy z witryny do witryny, przypisywane są do nas pliki cookie – ciasteczka. Ciasteczka to elementy pozwalające identyfikować naszą cyfrową tożsamość na wielu witrynach.

Ich zaletą jest to, że pozwalają dostarczać nam odpowiednich treści, niekiedy wręcz warunkują funkcjonowanie spersonalizowanych usług. A wadą jest to, że niemal automatyczne akceptowanie przez nas ustawień prywatności serwisów oznacza zgodę na personalizowanie reklam.

W efekcie gdy na przykład rozglądamy się za nowym laptopem, już po krótkim wyszukiwaniu takiego sprzętu, odwiedzając jakikolwiek serwis zawierający reklamy Google AdSense, będziemy widzieć właśnie reklamy laptopów.

Automatyzacja i algorytmy śledzące

Bardzo prężnie rozwija się technologia pozwalająca na automatyczne profilowanie użytkowników. Na podstawie zebranych na ich temat informacji są im przedstawiane takie treści, które mają sprawić, że z większym prawdopodobieństwem kupią dany produkt. Oto przykład, jak to działa. Na jednej stronie wypełniamy ankietę, na przykład by skorzystać z promocji czy wziąć udział w konkursie – podajemy w niej jakieś wydawałoby się mało charakterystyczne dane, jak wiek, płeć, zainteresowania. Następnie na innej stronie kupujemy lot samolotem na wakacje. Potwierdzenie płatności zostanie wysłane na nasz adres e-mail na przykład w usłudze Gmail. A potem automatycznie będziemy dostawać przypomnienia, że zbliża się nasz wylot. Zaczniemy otrzymywać mnóstwo reklam związanych z wyjazdem, a nawet z miejscem docelowym. Oprócz tego, jeśli algorytm stwierdzi na podstawie historii

WAŻNE INFORMACJE, KTÓRE TAKŻE MOGĄ WYCIEC

Wrażliwe dane dotyczące finansów czy zdrowia na szczęście wyciekają rzadko, przyjmuje się, że dotyczy to jednego na stu użytkowników internetu. Są to jednak bardzo ważne dane.

BĄDŹMY BEZPIECZNI W INTERNECIE

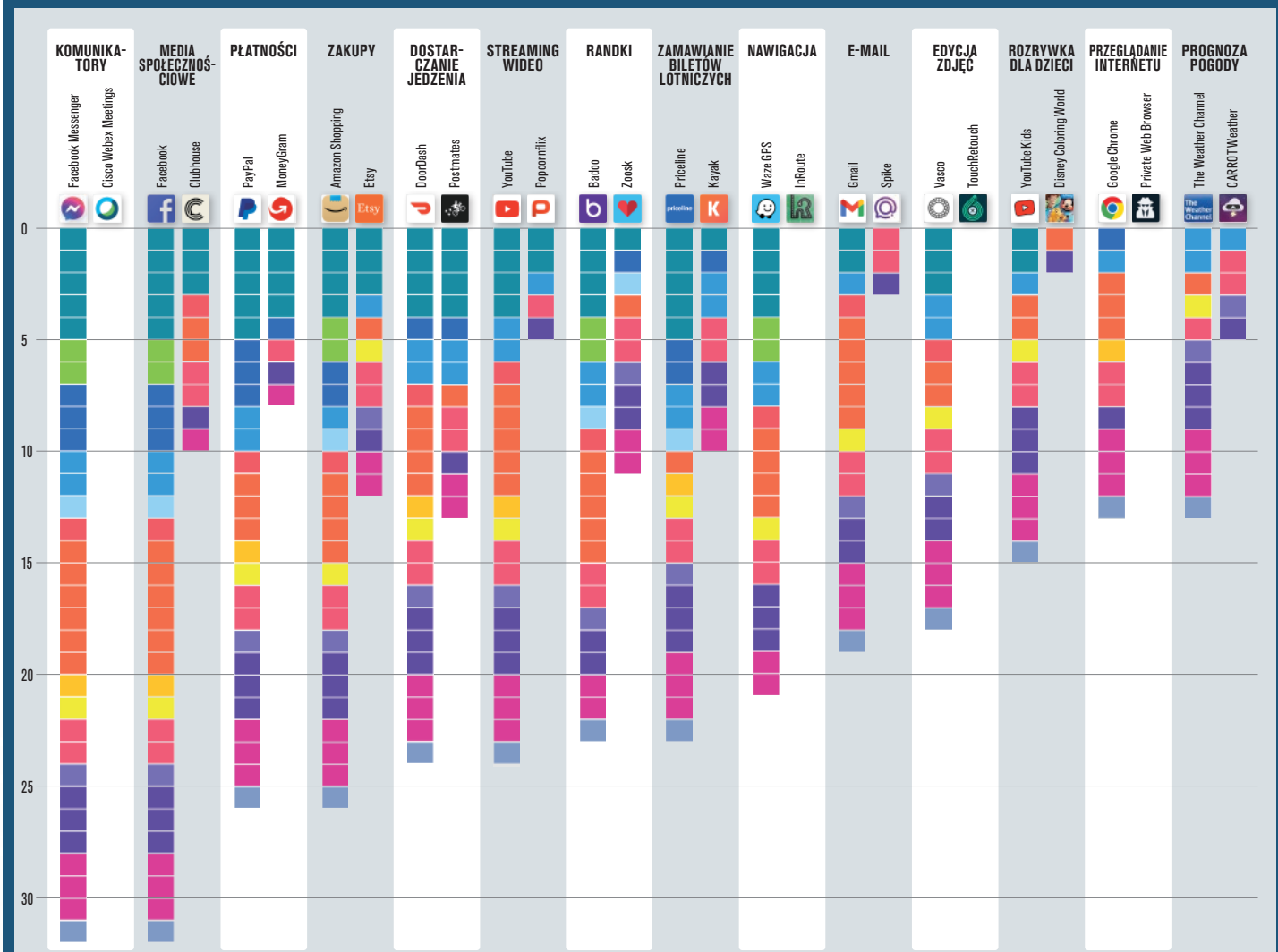
Jeśli nie chcemy, aby wyciek naszych danych doprowadził do poważnych kłopotów, starajmy się stosować do tych zasad:

- Korzystamy z menedżerów haseł i używamy różnych haseł do różnych serwisów
- Jeśli to możliwe, korzystamy wszędzie z autoryzacji dwuskładnikowej
- Korzystamy z VPN-u, programów antywirusowych oraz firewalli
- Do płatności online najlepiej jest wykorzystywać karty z możliwością doładowania lub wirtualne, jak na przykład Revolut.
- Unikamy klikania na podejrzane linki, zwłaszcza takie, które nie mają pełnej postaci (skrócone).
- Korzystajmy z szyfrowanych aplikacji – chmury, komunikatora
- Zgłaszamy do odpowiednich służb, jeśli staniemy się ofiarą cyberataku

PARTNER WYDANIA:
Surfshark®

JAKIE DANE I ILE ZBIERAJĄ POPULARNE APLIKACJE

Poniższe zestawienie, na przykładzie aplikacji, które zbierają najwięcej i – dla porównania – najmniej danych o swoich użytkownikach, pokazuje, jak dużo różnorodnych informacji o nas przechwytują popularne usługi. Zestawienie to zostało stworzone na podstawie źródeł dostępnych w Apple Store. Wynika z niego, że najwięcej danych pobierają aplikacje społecznościowe i apki do dostarczania jedzenia, a najmniej – przeglądarki i edytory zdjęć. Ogólnie najpopularniejsze aplikacje (czyli te, które mają najwięcej pobrań) zbierają najwięcej prywatnych danych z największej liczby kategorii. A trzy aplikacje z największym apetytem na dane należą do Fecebooka – są to: Facebook, Instagram, Messenger. Aplikacje, które zbierają najmniej informacji, zwykle zostały stworzone z myślą o prywatności, ale są mało popularne.



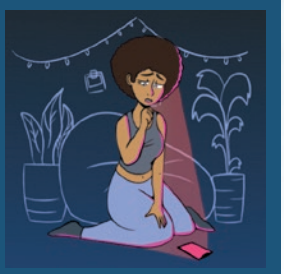
TYPY ZBIERANYCH DANYCH

- Dane kontaktowe
- Wrażliwe dane
- Historia wyszukiwania
- Dane diagnostyczne
- Zdrowie i fitness
- Kontakty
- Dane osobowe
- Inne
- Informacje finansowe
- Zawartość tworzona przez użytkowników
- Dane dotyczące zakupów
- Lokalizacja
- Historia przeglądania
- Dane dotyczące użytkowania

Fot. Chainarong Prasertthai, Shutter2U/iStockphoto.com

WYCIEK DANYCH – TO SIĘ MOŻE ZDARZYĆ KAŻDEMU

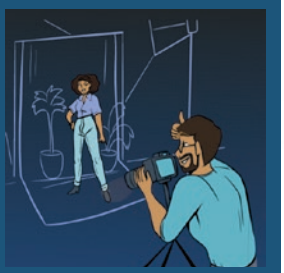
▪ INFLUENCER W MEDIACH SPOŁECZNOŚCIOWYCH



Wyciek danych dotyczy: dane osobowe, ID konta, hasło

Nasz przykładowy influencer zarabia na życie swoją reputacją i tym, co umieszcza na swoim profilu społecznościowym. Atakujący, wykorzystujący ogólnodostępne bazy z różnych wycieków, uzyskali wymienione powyżej informacje. Okazały się one wystarczające do całkowitego przejęcia kontroli nad kontem w serwisie społecznościowymm. W celu odzyskania dostępu do konta jego właściciel musiał zapłacić okup – na szczęście atakujący nie wykorzystali konta do bardziej złośliwych działań i nie usunęli jego zawartości. Pamiętajmy, by dbać o to, aby nasze hasła były jak najbardziej unikalne i złożone.

▪ FOTOGRAF



Wyciek danych dotyczy: prywatny adres e-mail, hasło

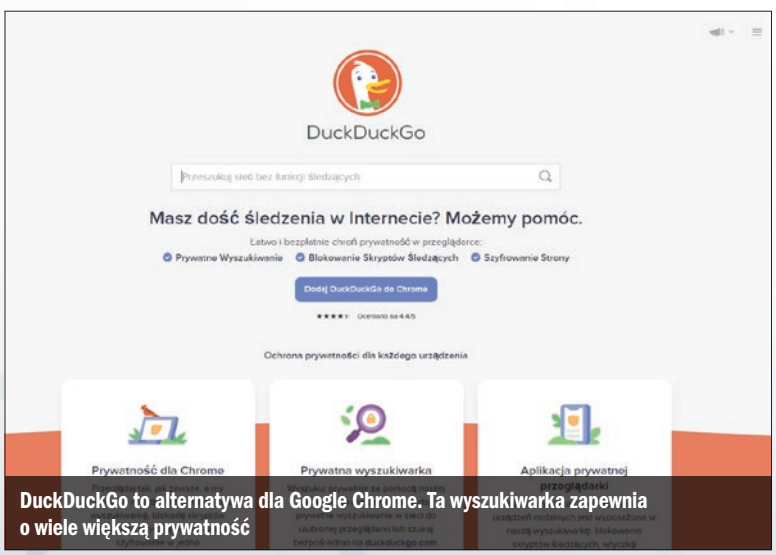
Nasz przykładowy fotograf prowadzi prywatną stronę, poprzez którą utrzymuje kontakt ze swoimi klientami i na której prezentuje swoje dzieła. Tworzył ją kilka lat i zapracował na zaufanie sporego grona osób. Hakerzy zdobyli jego dane, które zostały udostępnione w wycieku. Uzyskali dostęp do jego strony i zaczęli sprzedawać fikcyjne produkty. Klienci wpłacali kwoty na konto hakerów, wierząc, że otrzymają zamówione produkty. Fotografowi zajęło wiele czasu na odzyskanie kontroli nad stroną. W tym czasie hakerzy oszukali wielu klientów i zepsuli mu opinię. Przyczyną problemów było to, że fotograf wykorzystywał to samo hasło i adres e-mail do wielu swoich kont, z jakich korzystał w internecie. Atakujący przejęli kontrolę nad wszystkimi usługami, z jakich korzystał, w tym nad prywatną pocztą oraz stroną internetową.

naszych zakupów i naszego wieku, że raczej nie dysponujemy dużymi kwotami, będziemy widywali reklamy poradników turystycznych i gadżetów. Reklamy gadżetów mogą być dopasowane do naszej płci. A jeśli automat oceni, że mamy znacznie zasobniejszy portfel, co też widać w historii zakupów, będziemy otrzymywać reklamy luksusowych hoteli, wypożyczalni samochodów itp. Część użytkowników może stwierdzić, że jest to wygodne, że dzięki takim mechanizmom życie staje się prostsze. Tylko że kosztem tej wygody są nasze prywatne dane kupowane przez korporacje, które starają się sprzedać jak najwięcej swoich produktów.

Prywatne wyszukiwanie w sieci

Jeśli nie chcemy, aby wyszukiwarka Google zbierała o nas dane, warto zacząć korzystać ze znacznie bardziej anonimowej wyszukiwarki, na przykład DuckDuckGo. Jest ona dostępna jako dodatek do wielu popularnych przeglądarek i można ją pobrać jako aplikację mobilną na smartfon. Nie zbiera naszych wyników wyszukiwania i ma wbudowany dodatek, który wymusza szyfrowanie oraz blokuje skrypty śledzące – zwiększa to nasze bezpieczeństwo i prywatność w internecie.

Najważniejszy zapis polityki prywatności DuckDuckGo to: „Nie gromadzimy ani nie udostępniamy żadnych informacji o naszych użytkownikach".



DuckDuckGo to alternatywa dla Google Chrome. Ta wyszukiwarka zapewnia o wiele większą prywatność

Ciekawą opcją jest możliwość automatycznego czyszczenia danych przeglądania po określonym czasie braku aktywności użytkownika.

Co się dzieje, gdy wyciekną prywatne dane

Publicznie dostępne bazy danych najczęściej zawierają adresy e-mail, hasła, ID kont, hashe haseł oraz adresy IP.

Wykres na 3 stronie przedstawia, ile jakich typów danych znajduje się w wyciekach danych w przeliczeniu na 100 użytkowników internetu.

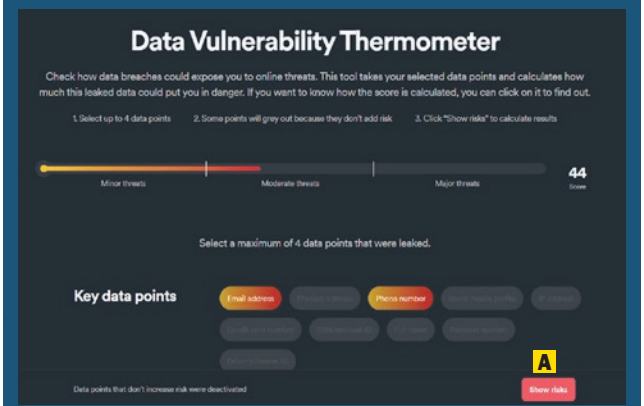
Zdecydowanie najczęściej dochodzi do wycieku samego adresu e-mail użytkownika. Statystycznie adres e-mail każdego użytkownika internetu może wyciec dwa, trzy razy. Przyczyną jest to, że rejestrujemy się na wielu różnych witrynach, w newsletterach, usługach itp., w większości przypadków podając zawsze ten sam e-mail. I jeśli dojdzie do wycieku danych z różnych serwisów, ten sam adres trafia do różnych publicznych baz zawierających prywatne dane użytkowników internetu.

Nieco rzadziej dochodzi do wycieku haseł użytkowników sieci. Przyjmuje się jednak, że średnio dwa hasła jednego użytkownika znajdują się w ogólnodostępnych bazach.

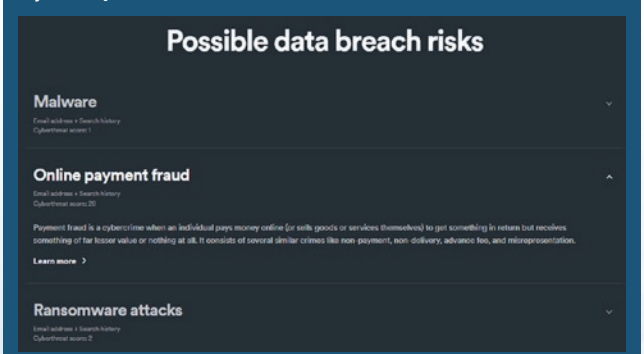
SAM SPRAWDŹ, CO MOŻE CI GROZIĆ

Korzystając z narzędzia na stronie o adresie: surfshark.com/research/data-breach-impact możemy dla czterech wybranych danych sprawdzić, co może nam grozić, jeśli znajdą się one w niepowołanych rękach.

1 Zaznaczamy odpowiednie pola z opisami danych i klikamy na Show risks **A**.



2 Po chwili zostanie wyświetlona lista różnego typu ataków, na które możemy być narażeni, jeśli zaznaczone przez nas dane wycieką.



Mogłoby się to wydawać niezbyt ryzykowne. Jeśli jednak potencjalni atakujący sparują nasz adres e-mail z hasłem z wycieku na jednej stronie, mogą użyć tych danych na innych naszych kontach. Dlatego tak ważne jest tworzenie osobnych haseł do osobnych kont.
Zdecydowanie rzadziej wyciekają unikalne ID kont, na przykład do serwisu Steam i tym podobnych. Podobnie hashe haseł, a najrzadziej dochodzi do wycieku unikalnych adresów IP. Jedynie w wypadku 19 na 100 użytkowników sieci został udostępniony publicznie taki adres.

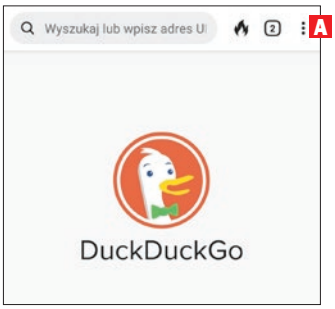
Prywatność na smartfonie

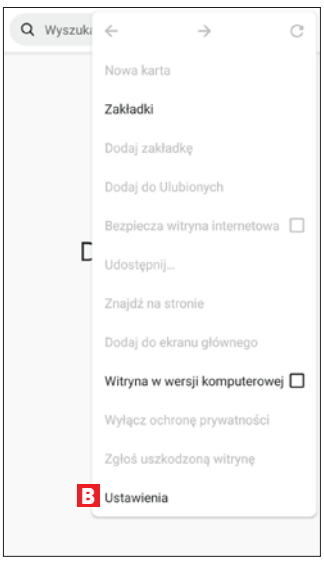
Najczęstszą drogą wycieków prywatnych danych z urządzeń mobilnych są aplikacje, których używamy na co dzień.
Kiedy pobieramy darmową aplikację z dedykowanego sklepu, jej twórcy wymagają od nas różnego rodzaju zgód i dostępu do uprawnień. W następstwie mogą uzyskać dostęp do wielu informacji i do naszych danych, które potem mogą na przykład odsprzedać innym firmom czy reklamodawcom. Badania wykonane na Uniwersytecie w Oksfordzie w 2018 roku wskazują, że średnio jedna aplikacja może sprawić, że nasze dane trafią aż do 10 firm.
Nawet z pozoru mało istotne informacje, jak choćby nawyki dotyczące korzystania z aplikacji, nasza lokalizacja, wiek czy płeć, pozwalają firmom dopasować do nas odpowiedni profil reklamowy.
Firma Apple jakiś czas temu udostępniła etykiety dotyczące prywatności (ang. Privacy Nutrition Labels). Pokazują one, jak wiele i jak rożnorodne informacje o nas pozyskują aplikacje mobilne (patrz wykres na stronie 3).

DUCKDUCKGO PRIVACY BROWSER: KONFIGURACJA I KORZYSTANIE

Aby korzystać z DuckDuckGo na komputerze, wystarczy dodać dodatek do przeglądarki, na smartfonie trzeba zainstalować aplikację. Przyjrzyjmy się bliżej przeglądarce dostępnej na smartfony – warto wiedzieć, jak korzystać z jej funkcji ważnych dla prywatności.

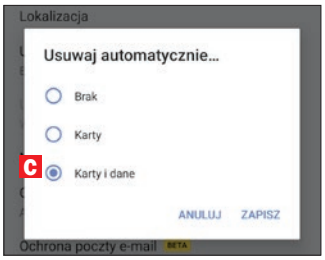
1 Po uruchomieniu przeglądarki możemy od razu aktywować funkcję automatycznego czyszczenia danych. W głównym oknie aplikacji naciskamy trzy kropki **A** w prawym górnym rogu, a następnie **Ustawienia** **B**.



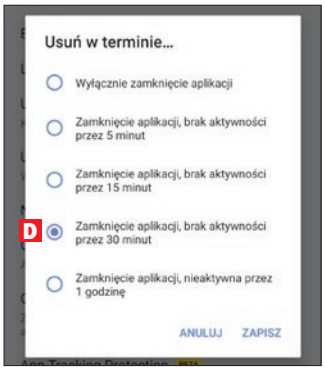


2 W ustawieniach naciskamy **Usuwaj automatycznie**, wybieramy opcję **Karty i dane** **C** i naciskamy **Zapisz**.

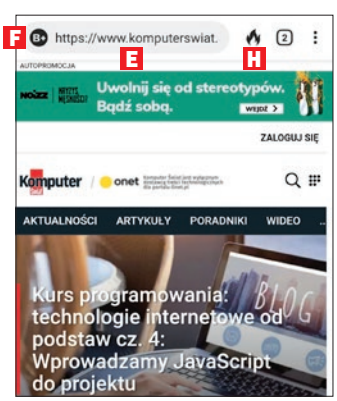
3 Następnie naciskamy **Usuń w terminie**. Wybieramy odpowiadającą nam opcję **D**. Na koniec naciskamy **Zapisz**.



4 Z aplikacji możemy korzystać jak z innych przeglądarek. Na górnym pasku **E** można wyszukiwać różne frazy lub wpisywać bezpośrednio adresy stron.

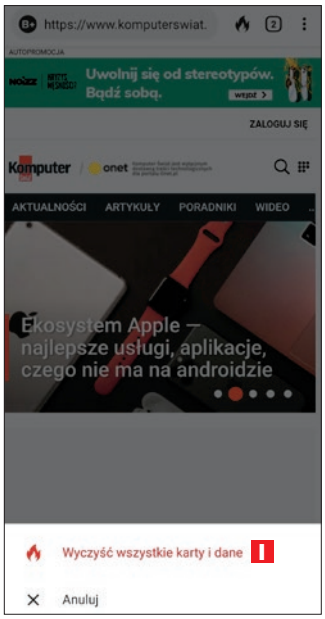


5 Po przejściu na dowolną stronę zobaczymy w lewym górnym rogu ocenę jej prywatności **F**. Po kliknięciu na tę ocenę możemy zapoznać się ze szczegółami **G**. Na przykład witryna komputerswiat.pl uzyskała ocenę **B+**, jest to wysoka ocena. Dzięki systemowi ocen prywatności DuckDuckGo jest w stanie szybko podać informacje na temat ochrony prywatności na konkretnej witrynie. Dzięki temu, odwiedzając daną stronę, od razu wiemy, czy możemy czuć się bezpiecznie.



Czyszczenie sesji w DuckDuckGo Privacy Browser

W celu szybkiego wyczyszczenia sesji i wszystkich danych przeglądania wystarczy nacisnąć ikonę płomienia **H** po prawej stronie paska adresowego. Następnie naciskamy **Wyczyść wszystkie karty i dane** **I**. Pojawi się animacja płomieni i wszystkie dane przeglądania zostaną usunięte.



SURFSHARK – VPN DLA KAŻDEGO

Nikogo nie trzeba przekonywać, że bezpieczeństwo i prywatność mają kluczowe znaczenie. ***Jednym z najlepszych sposobów na ochronę prywatności jest korzystanie na stałe z usługi VPN****. Program Surfshark VPN zapewnia najwyższy poziom bezpieczeństwa, jest wygodny i działa skutecznie. Poznajmy go*

Surfshark pojawił się na rynku VPN w roku 2018. W ciągu zaledwie roku firma uruchomiła ponad 1700 serwerów w 63 krajach świata.

Dziś liczba serwerów Surfshark wynosi ponad 3200 w 65 krajach. To ważna informacja. Im bogatsza jest infrastruktura usługodawcy, tym więcej wirtualnych lokalizacji mają do wyboru użytkownicy korzystający z VPN-u, którzy chcą zachować bezpieczeństwo i anonimowość podczas surfowania.

Warto też wiedzieć, że Surf shark ma siedzibę na Brytyjskich Wyspach Dziewiczych (BWD). Choć jest to terytorium zamorskie Zjednoczonego Królestwa, to BWD mają własne prawo. Nie ma tam prawnie wymuszanych mechanizmów ujawniania danych przez operatorów internetowych.

Oznacza to, że Surfshark może działać w pełni anonimowo z poszanowaniem litery prawa – nikt nie może żądać od usługodawcy ujawnienia danych użytkowników.

Zresztą nie jest to możliwe ze względów technicznych – serwery Surfshark nie przechowują danych na trwałych nośnikach, przetwarzanie danych odbywa się w pamięci RAM serwerów, a jak wiadomo – jest to pamięć ulotna. Wystarczy odłączenie zasilania i po danych nie ma śladu.

Warte uwagi funkcje Surfshark VPN

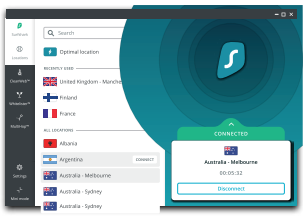
Oprócz dostępnego w usłudze Surfshark VPN bezpiecznego szyfrowania otrzymujemy dostęp do wielu zaawansowanych i unikalnych rozwiązań, które znacznie zwiększają bezpieczeństwo i wygodę korzystania z programu typu VPN.

DODATKOWE ZALETY SURFSHARK VPN

- Dostępne rozszerzenia dla popularnych przeglądarek (Chrome, Firefox)
- Działa na urządzeniach mobilnych
- Obsługuje współdzielenie plików wsieciach P2P
- Pomoc techniczna wformie czatu dostępna 24/7
- Polityka braku logów uniemożliwiająca identyfikację jakiegokolwiek użytkownika usługi
- Bardzo mocne szyfrowanie (algorytm AES-256-GCM)

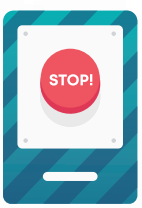
Oto niektóre z nich:

- **CleanWeb** – funkcja, która umożliwia blokowanie malware'u, zanim zostanie załadowany na stronach internetowych, oraz reklam. Pozwala to oszczędzić pobierane dane, co ma znaczenie, jeśli korzystamy z planu taryfowego. Dodatkowo moduł ten pozwala na znacznie szybsze ładowanie stron i serwisów.



- **Nieograniczona ilość urządzeń** – korzystając z jednego konta, możemy zalogować się nim na nieograniczonej ilości urządzeń. Większość usług typu VPN pozwala na jednym koncie skorzystać z jednego bądź kilku urządzeń. Surfshark nie narzuca żadnych ograniczeń. Jeśli mamy wiele urządzeń, możemy sporo zaoszczędzić.

- **Bypasser** – to funkcja dzielonego tunelowania, pozwala na dzielenie ruchu sieciowego i przepuszczanie części ruchu przez VPN i szyfrowane połączenie, a części ruchu – bez tunelowania VPN. Jednocześnie korzystamy z dwóch adresów IP. Ma to znaczenie, na przykład gdy nasz bank zabrania korzystania z serwisów typu VPN.



- **Kill Switch** – ta funkcja umożliwia automatyczne zablokowanie połączenia sieciowego, jeśli w trakcie pracy programu Surfshark przestanie poprawnie działać nasz tunel VPN. Dzięki temu nawet na chwilę nie zostaniemy w sieci bez ochrony VPN-u.

- **Camouflage Mode** – ta funkcja umożliwia maskowanie naszego połączenia w taki sposób, aby nawet nasz dostawca internetu nie był w stanie zweryfikować tego, czy korzystamy z usług VPN, czy też nie.

- **Change your IP** – dzięki tej opcji możemy dowolnie zmieniać nasz zewnętrzny adres IP, a tym samym utrudnić namierzenie nas i powiązanie z konkretnymi zachowaniami.
- **Nexus** – jest to zestaw funkcji, których głównym zadaniem jest zwiększenie bezpieczeństwa użytkownika, możliwość zmiany adresu IP bez rozłączania usługi VPN, stabilizowanie i zwiększenie wydajności połączenia VPN.

Surfshark Nexus – rewolucja technologiczna w VPN-ie

Surfshark Nexus to jedno z ciekawszych rozwiązań na rynku VPN, które zostanie uruchomione w ciągu najbliższych lat – etapami.

Nexus to innowacja VPN-u oparta na technologii SDN (sieć definiowana programowo).

ZALETY NEXUSA

- Znacznie poprawia prywatność w internecie
- Zezwala na zmianę adresu IP wsieci bez odłączania od VPN-u
- Oferuje nowe funkcje, które zwiększają prywatność
- Stabilizuje iprzyspiesza połączenia VPN zarówno lokalnie, jak i za granicą

W przeciwieństwie do wszystkich innych sieci VPN, które po prostu kierują użytkownika do wybranego serwera VPN (a nie do sieci), Nexus umożliwia łączenie z całą siecią serwerów i kieruje do wybranej lokalizacji.

„Sieci serwerów", o których mówi większość producentów rozwiązań VPN, nie są tak naprawdę sieciami i powinny być raczej nazywane „listą serwerów do wyboru".

Nexus to prawdziwa sieć.

Jak Nexus rozwiązuje problemy tradycyjnych usług VPN

Problemy tradycyjnych VPN-ów

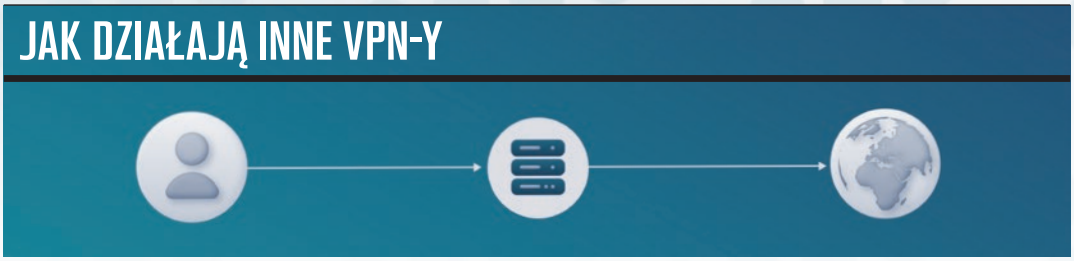
Tradycyjne usługi VPN działają, tworząc zaszyfrowany tunel między urządzeniem a serwerem VPN. Po nawiązaniu połączenia uzyskujemy dostęp do internetu za pośrednictwem serwera VPN, który zmienia nasz widoczny adres IP.

Ten tunel jest następnie używany do wejścia do internetu (połączenia) i wyjścia z internetu, zapewniając warstwę ochrony cybernetycznej, czyli ukrywając prawdziwą lokalizację użytkownika poprzez pokazywanie innego adresu IP niż ten dostarczony przez dostawcę usług internetowych, a także szyfrując ruch.

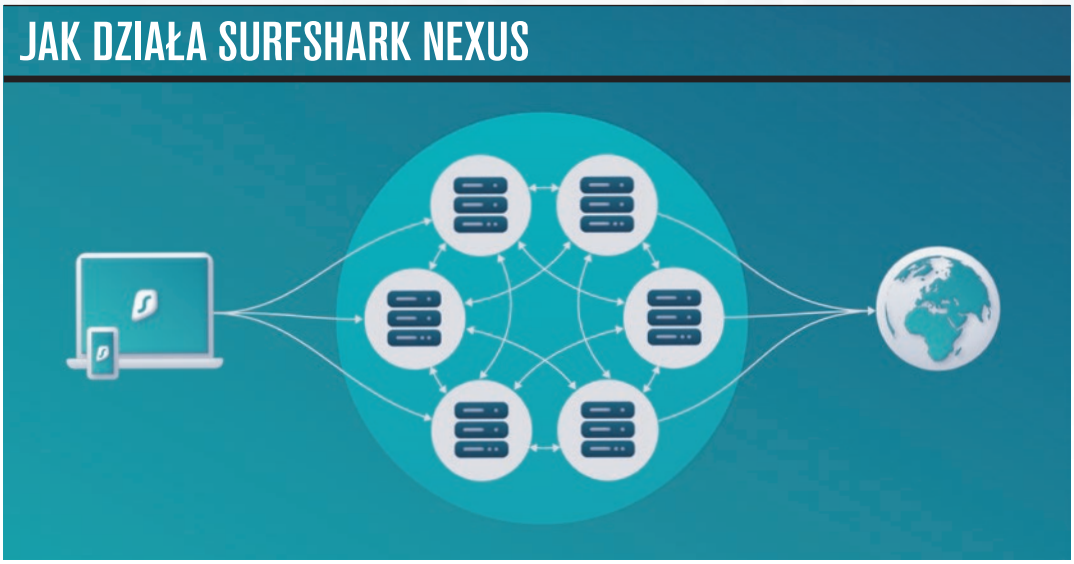
Niestety, na tym etapie pojawia się kilka problemów:

- Otrzymany adres IP pozostaje taki sam. Po połączeniu z serwerem VPN prawdziwy adres IP użytkownika jest ukryty, ale jego aktywność w internecie jest nadal związana z jednym adresem IP. Jeśli z jakiegoś powodu ktoś zbiera informacje o tej aktywności, zwiększa to szanse na rozpoznanie ukrywającego się użytkownika.
- Nie można wiele zrobić dla poprawy wydajności połączenia VPN. Połączenie międzynarodowe, a zwłaszcza na duże odległości, pogarsza szybkość i stabilność łącza. Ponadto, jeśli łączymy się z przeciążonym serwerem, dostawca VPN-u nie może nic zrobić, aby go przyspieszyć, bez odłączania swoich użytkowników.
- Awarie serwera, konserwacja lub połączenia na duże odległości mogą spowodować odłączenie od sieci VPN. Bezpośrednie połączenie sprawia, że użytkownik jest całkowicie zależny od stanu serwera VPN. Jeśli połączenie zostanie z jakiegoś powodu przerwane, może to pozostawić użytkownika bez ochrony i ujawnić jego dane.

JAK DZIAŁAJĄ INNE VPN-Y



JAK DZIAŁA SURFSHARK NEXUS



Rozwiązania problemów oferowane przez Nexusa

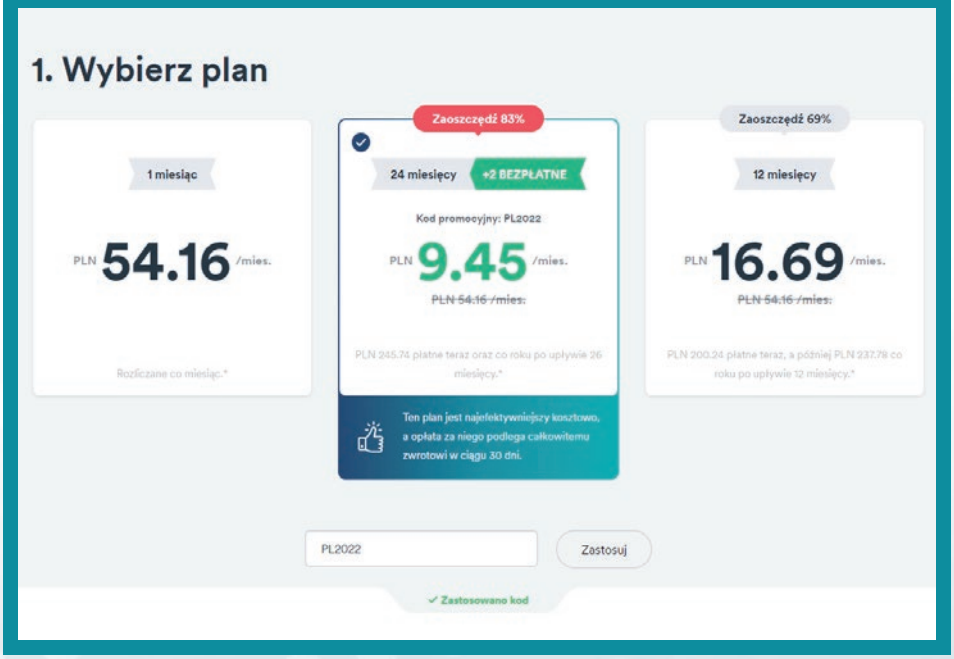
Połączenie wszystkich serwerów w jedną, zdefiniowaną programowo sieć, nazwaną Nexus, umożliwia wprowadzenie nowych funkcji, które rozwiązują problemy użytkowników tradycyjnych VPN-ów:

- **IP Rotator** – ta funkcja rozwiąże problemy dotyczące prywatności, związane z posiadaniem tego samego adresu IP po połączeniu z VPN-em przez długi czas. Automatycznie zmienia adres IP bez odłączania użytkownika od VPN-u. Pozwala wybrać sposób rotacji adresu IP – w określonej lokalizacji, kraju, regionie, a nawet na całym świecie.
- **IP Randomizer** – ta funkcja ukryje wzorce przeglądania właściwe dla użytkownika. Po włączeniu nadaje urządzeniu nowy adres IP za każdym razem, gdy użytkownik odwiedza inną witrynę (lub inny zasób internetowy). Dwadzieścia różnych zakładek w przeglądarce to dwadzieścia różnych adresów IP.
- **Dynamic HultiHop** – ta funkcja pozwala na wybranie własnych lokalizacji wejścia i wyjścia w dowolny sposób. Można połączyć się przez Austrię ze Stanami Zjednoczonymi, a następnie przełączyć się na Singapur.
- **Lepsze prędkości.** Nexus pozwala na połączenie z najwydajniejszymi (w większości przypadków najbliższymi) serwerami wejściowymi i umożliwi wyjście z dowolnej lokalizacji. To rozwiąże wiele międzynarodowych i lokalnych problemów z szybkością internetu.
- **Lepsze połączenie.** Optymalizacja połączenia i wydajności sieci oraz przeprowadzanie konserwacji w większości przypadków odbywa się bez odłączania użytkowników od VPN-u. Dzięki temu użytkownicy zyskują bardziej stabilne połączenia i lepszą ochronę przed wyciekami DNS i pakietów danych.
- **Lepsza wydajność VPN-u.** Sieć serwerów pozwala na kierowanie ruchu sieciowego na podstawie przypisanych do użytkownika wzorców ruchu, takich jak przesyłanie strumieniowe, pobieranie lub przeglądanie. Poprawi to wydajność połączenia. **Zastrzeżenie:** Nie oznacza to, że nasza aktywność jest śledzona.

Warto wiedzieć: Obecnie można korzystać z funkcji **IP Rotator**, która umożliwia automatyczną zmianę adresu IP co 10 minut, bez przerw w połączeniu i bez zaangażowania użytkownika. Kolejne funkcje będą udostępniane w następnych aktualizacjach stopniowo w latach 2022 i 2023.

RABAT DLA CZYTELNIKÓW KOMPUTER ŚWIATA

Czytelnicy Komputer Świata otrzymują specjalny rabat. Kod zniżkowy **PL2022** trzeba wpisać na stronie **surfshark.com** przy kasie. Kod daje 83 procent zniżki i dwa miesiące gratis przy zakupie planu na dwa lata.



Fot. Shutter2U/iStockphoto.com

RABAT 83%
DLA CZYTELNIKÓW
Każdy Czytelnik, który zdecyduje się na zakup Surfshark VPN w planie na 2 lata, może skorzystać z kodu rabatowego na stronie surfshark.com
KOD: PL2022
Realizacja kodu w koszyku

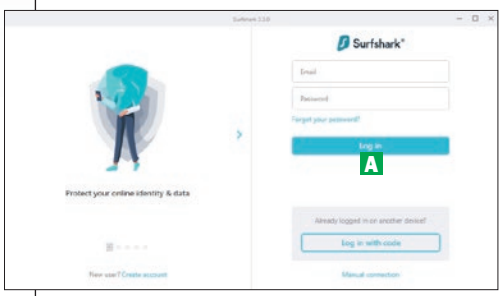
VPN NA KOMPUTERZE I SMARTFONIE

Zachowanie prywatności powinno być dla nas ważne, zarówno gdy korzystamy z internetu na komputerze, jak i na smartfonie. Przeczytajmy zatem, jak prawidłowo korzystać z usług VPN na tych urządzeniach – na przykładzie **Surfshark VPN**. Jest on dostępny do kupienia na stronie **surfshark.com** w planach: na miesiąc, na rok i na dwa lata.

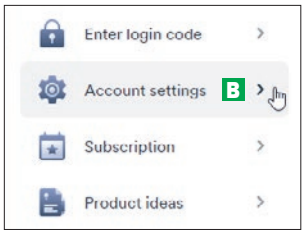
ANONIMOWY DOSTĘP DO INTERNETU NA KOMPUTERZE

Zacznijmy od konfiguracji usługi Surfshark VPN na komputerze z systemem Windows. Aby wykupić usługę, należy odwiedzić stronę o adresie **surfshark.com**. Jeśli zdecydujemy się na plan dwuletni, będziemy mogli skorzystać z rabatu i miesiąc korzystania z VPN-u będzie nas kosztować około 9,5 złotego.

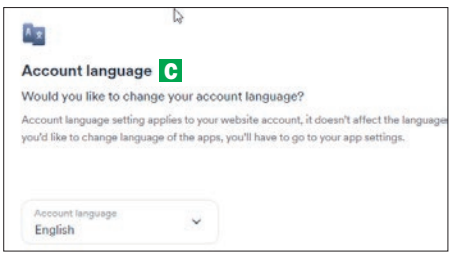
1 Po zakończeniu procesu zakupowego logujemy się na nasze konto A. Zostaniemy przeniesieni do widoku **Setup guides**.



2 Klikamy w prawym górnym rogu na nasz login i z menu wybieramy opcję **Account settings** B.

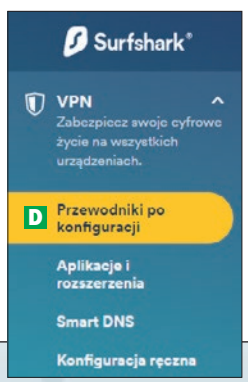


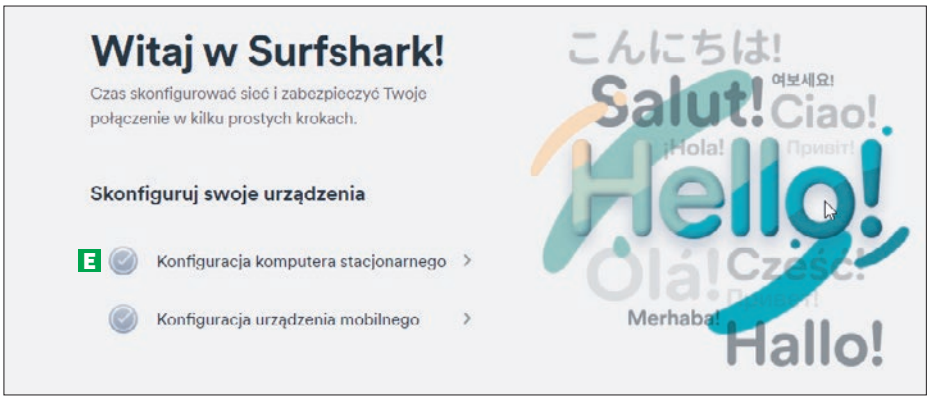
3 Następnie w sekcji **Account language** C wybieramy z listy język polski i po chwili interfejs naszego konta będzie dostępny w języku polskim.



4 Po dokonaniu zmiany klikamy po lewej stronie na **VPN**, a następnie na **Przewodniki po konfiguracji** D.

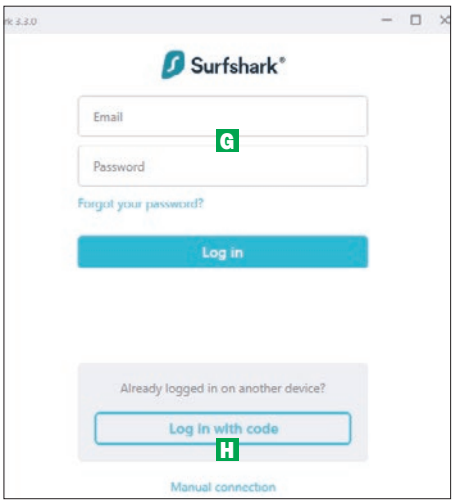
5 Teraz klikamy na **Konfiguracja komputera stacjonarnego** E.



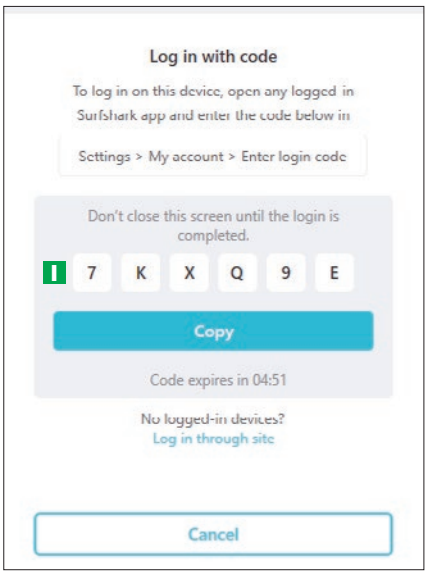


6 Rozpoczynamy od kliknięcia na **Pobierz aplikację na komputer** F.

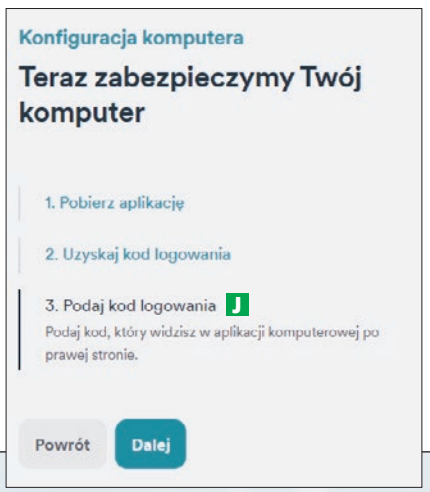
7 Po pobraniu programu instalujemy go i uruchamiamy. Możemy się zalogować, podając adres e-mail i hasło G. Możemy również kliknąć na **Log in with code** H.



8 W tym drugim wypadku w kolejnym oknie pojawi się sześcioznakowy kod I, który należy podać na stronie, klikając na **Podaj kod logowania** J.



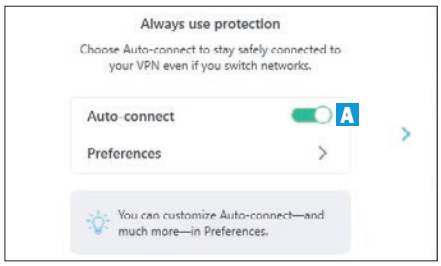
9 Po wprowadzeniu kodu klikamy na **Dalej** i zostajemy automatycznie zalogowani.



PIERWSZE KROKI

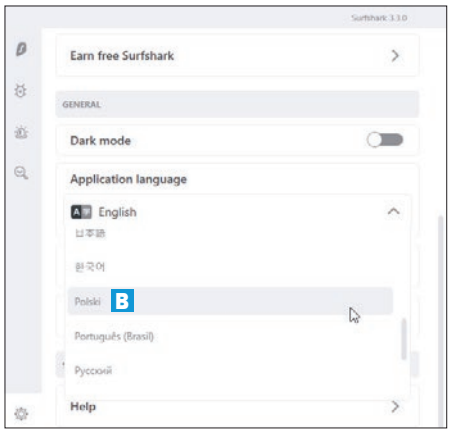
Od razu po zalogowaniu pojawi się wstępny kreator, który pozwoli nam skonfigurować program Surfshark do pracy.

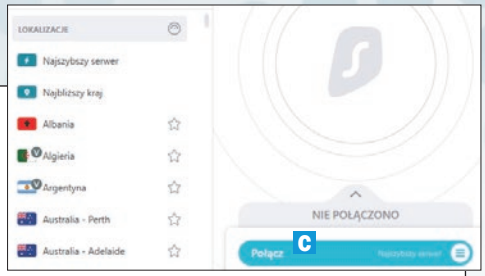
1 W pierwszym oknie aktywujemy usługę **Auto-connect** A, dzięki temu będziemy połączeni z usługą VPN od razu po uruchomieniu systemu. W kolejnych dowiemy się o podstawowych możliwościach programu.



2 Po pojawieniu się głównego okna programu po lewej stronie klikamy na **Settings**.

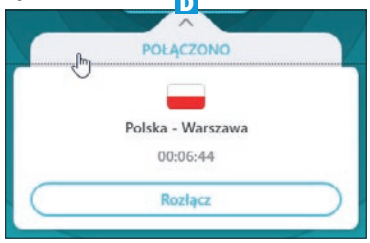
3 Następnie w kategorii **General**, w polu **Application Language** B wybieramy z listy język polski.





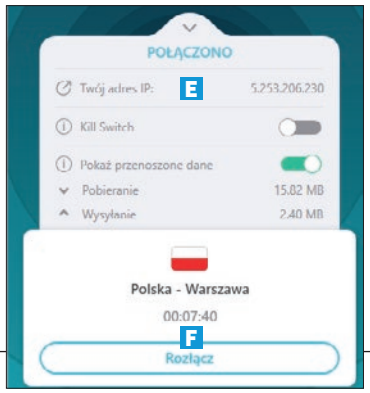
4 Teraz możemy rozpocząć właściwe korzystanie z aplikacji. W celu nawiązania połączenia VPN klikamy na **Połącz** C w prawym dolnym rogu.

5 Po chwili połączenie zostanie nawiązane. Automatycznie jest wybierany najszybszy serwer, pojawia się również informacja o lokalizacji serwera, z którym się łączymy – kraj oraz miasto.



6 Po kliknięciu na strzałkę D powyżej napisu **Połączono** poznamy szczegóły połączenia E, takie jak adres IP oraz informacje o łącznym transferze danych.

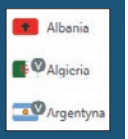
7 W celu zakończenia połączenia VPN należy kliknąć na **Rozłącz** F.



TO WARTO WIEDZIEĆ: WAŻNE IKONY SURFSHARKA

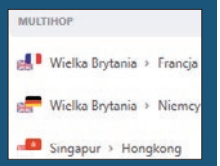
■ **Pokaż metryki prędkości** – po kliknięciu na ten przycisk, który znajduje się na pasku **Lokalizacje**, uzyskamy informacje na temat obciążenia każdego z serwerów oraz czasu odpowiedzi danego serwera. Im krótszy czas odpowiedzi, tym lepszej jakości będzie połączenie. Opóźnienie ma ogromne znaczenie zwłaszcza w przypadku, gdy chcemy grać w gry online typu FPS.

■ **Wirtualna lokalizacja** – niektóre serwery mają oznaczenie **V**. To wirtualna lokalizacja. Adresy IP wirtualnej lokalizacji pasują do kraju, z którym chcemy się połączyć, ale serwery mogą fizycznie znajdować się w innym miejscu. Co do zasady wirtualne lokalizacje zapewniają lepsze prędkości i większą niezawodność w przypadku sprawnej infrastruktury sieciowej.



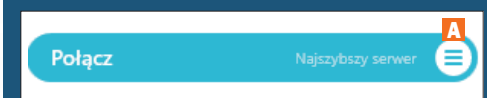
■ **Lokalizacja ze statycznym adresem IP** – niektóre serwery mają oznaczenie **S**. To serwery ze statycznym adresem IP, co oznacza, że nasz adres IP nie będzie zmieniany przy każdym połączeniu z danym serwerem. Ma to swoje wady i zalety, jednak z reguły dla większości użytkowników korzystniej jest wybierać pozostałe serwery.

■ **Lokalizacja Multi-Hop** – serwery, które są oznaczone dwiema flagami, to serwery typu MultiHop. Łączą nas one z docelowym serwerem przez dodatkowy serwer przesiadkowy. Takie rozwiązanie znacznie zwiększa bezpieczeństwo. Jednak należy zwrócić uwagę na opóźnienie, które może wystąpić przy tego typu połączeniach. Zwiększenie bezpieczeństwa odbywa się kosztem wydajności łącza.

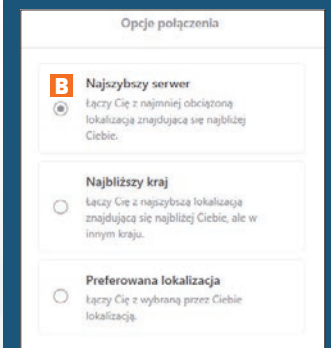


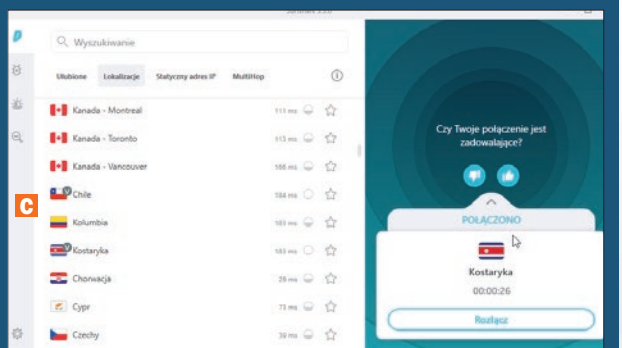
DOMYŚLNE POŁĄCZENIE

Klikając na trzy kreski A przy opcji **Połącz**, możemy wybrać rodzaj serwera, z jakim chcemy się połączyć.



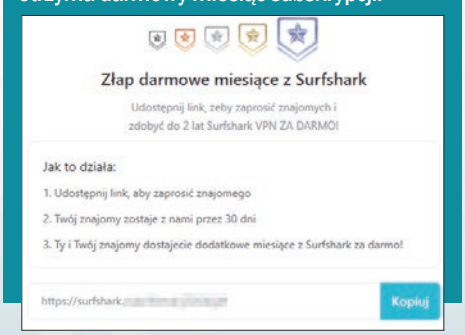
Domyślnie jest to opcja **Najszybszy serwer** B, możemy ją zmienić na **Najbliższy kraj** lub **Preferowana lokalizacja**.
Oczywiście możemy połączyć się z dowolnym serwerem w dowolnym kraju, wybierając z listy C w głównym oknie programu serwer, który nam odpowiada, i klikając na niego.





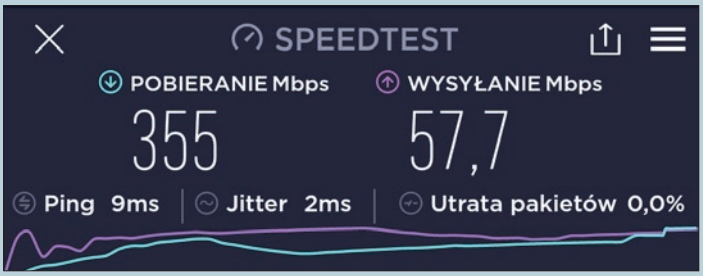
DARMOWE MIESIĄCE SUBSKRYPCJI

Warto wiedzieć: Jeśli weźmiemy udział w programie partnerskim Surfsharka, otrzymamy darmowy miesiąc subskrypcji. W tym celu należy udostępnić znajomemu specjalny link przypisany do naszego konta, a znajomy powinien wykupić subskrypcję i korzystać z programu przez minimum 30 dni. Znajomy także otrzyma darmowy miesiąc subskrypcji.

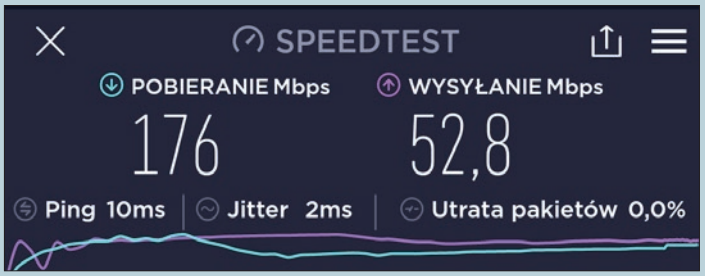


Wydajność połączenia przez VPN

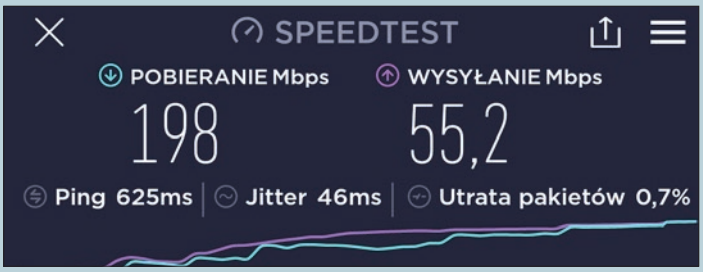
Oto kilka przykładów wydajności połączenia: bez usługi VPN, z usługą VPN i najbliższym serwerem, z usługą VPN i odległym serwerem, z usługą VPN i trybem MultiHop. Pomiary zostały wykonane za pomocą aplikacji Speedtest. Jak widać, wybór serwera ma ogromne znaczenie dla jakości połączenia. Jeśli nie jesteśmy zmuszeni korzystać z odległych serwerów z powodu na przykład blokad regionalnych, starajmy się wybierać serwery jak najbliższe naszej lokalizacji, które jednocześnie są najmniej obciążone.



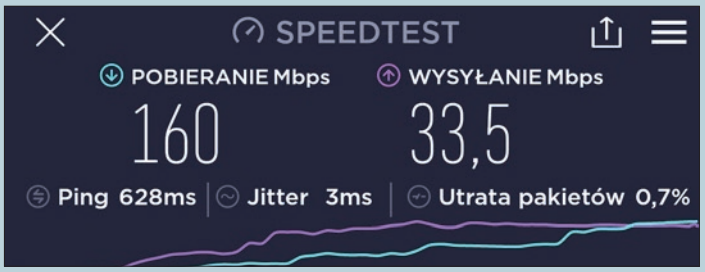
Dane kontrolne bez nawiązania połączenia VPN



Połączenie przez VPN z serwerem z najmniejszym opóźnieniem



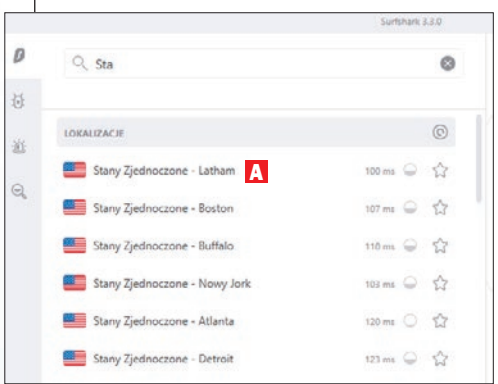
Połączenie przez VPN z serwerem z największym opóźnieniem – Australia



Połączenie przez VPN typu MultiHop do USA poprzez Australię

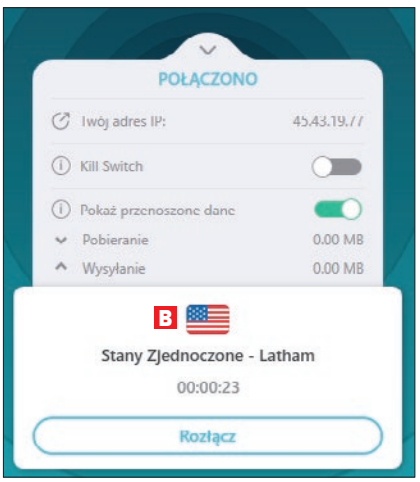
KORZYSTAMY Z SERWISÓW STREAMINGOWYCH W INNYCH KRAJACH

Jeśli zależy nam na dostępie do unikalnych seriali, które są dostępne na platformie streamingowej na przykład jedynie dla osób przebywających na terenie USA, możemy połączyć się z odpowiednim serwerem i korzystać z tego serwisu bez blokady regionalnej.

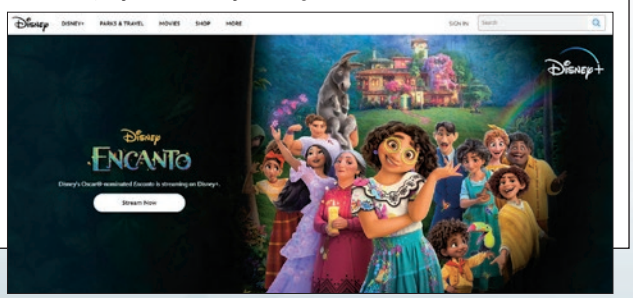


1 W głównym oknie programu Surfshark w polu wyszukiwania rozpoczynamy wpisywanie frazy **Stany**, po chwili zostaną wyświetlone wszystkie dostępne serwery z lokalizacji **Stany Zjednoczone** A. Wybieramy serwer z najniższym opóźnieniem i łączymy się z nim.

2 Po nawiązaniu połączenia uzyskamy nowy adres IP, który będzie wskazywać, że znajdujemy się w USA B.



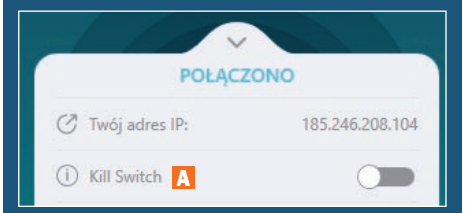
3 Teraz możemy wejść na stronę serwisu streamingowego – zostanie ona załadowana dla nas w taki sposób, jakbyśmy byli w danym kraju.



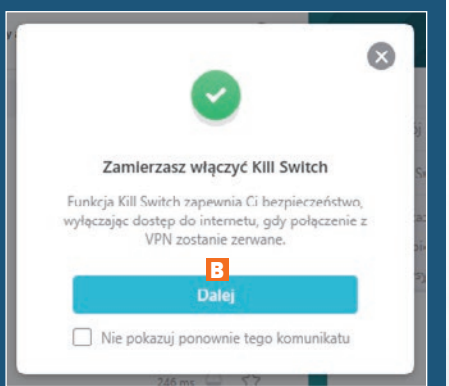
KILL SWITCH

Warto zabezpieczyć się na wypadek, gdyby nagle wystąpiły problemy sieciowe w trakcie aktywnego połączenia, i aktywować funkcję Kill Switch. Po jej aktywowaniu dostęp do internetu zostanie zablokowany, jeśli nie będziemy mieli aktywnego połączenia typu VPN. Dzięki temu nie będzie ryzyka, że będziemy nieświadomie korzystać z internetu bez VPN-u.

1 W celu aktywowania tej funkcji należy rozwinąć szczegóły połączenia i włączyć funkcję **Kill Switch** A.



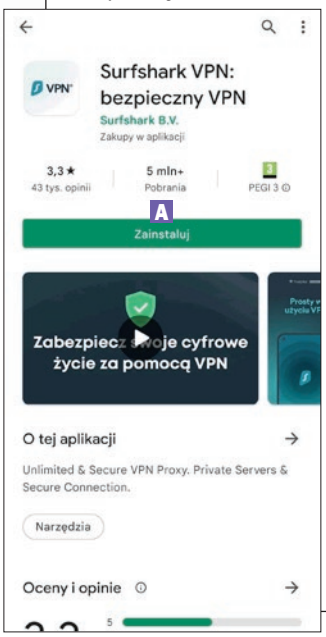
2 Następnie klikamy na Dalej B – funkcja Kill Switch zostanie aktywowana.



KORZYSTAMY Z SURFSHARK VPN NA SMARTFONIE

Zajmijmy się teraz konfiguracją usługi Surfshark VPN na smartfonie z Androidem (w przypadku smartfonów Apple procedura wygląda bardzo podobnie, jedyną różnicą jest to, że stosowną apkę pobieramy ze sklepu App Store, a nie z Google Play).

1 Zaczynamy od instalacji na smartfonie aplikacji **Surfshark VPN** A.



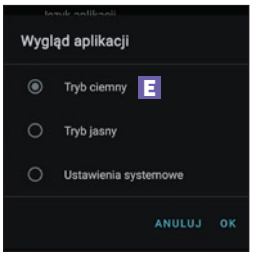
2 Następnie możemy rozpocząć 7-dniowy okres próbny. Jeżeli zarejestrowaliśmy konto i rozpoczęliśmy subskrypcję, naciskamy **Masz już konto? Zaloguj się** B.

3 Podajemy login oraz hasło i naciskamy **Zaloguj się**. Po pojawieniu się głównego widoku naciskamy **Połącz** C.

4 Potwierdzamy chęć nawiązania połączenia VPN na smartfonie, naciskając **OK**. Spowoduje to utworzenie automatycznej konfiguracji.

5 Dodatkowo zaleca się wyłączenie optymalizacji baterii dla Surfsharka – naciskamy **Wyłącz** D, potem zezwalamy aplikacji na pracę cały czas w tle. To konieczne, jeśli chcemy bez przeszkód i konieczności potwierdzania korzystać z VPN-u bez przerwy.

6 Jeżeli chcemy, możemy również zmienić motyw aplikacji na ciemny – przechodzimy do **Ustawień**, naciskamy **Wygląd aplikacji**, a potem **Tryb ciemny** E i **OK**.



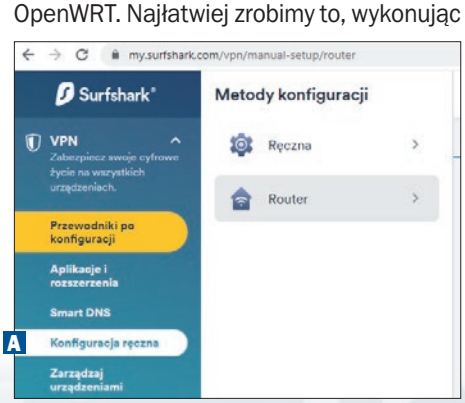
DLA ZAAWANSOWANYCH

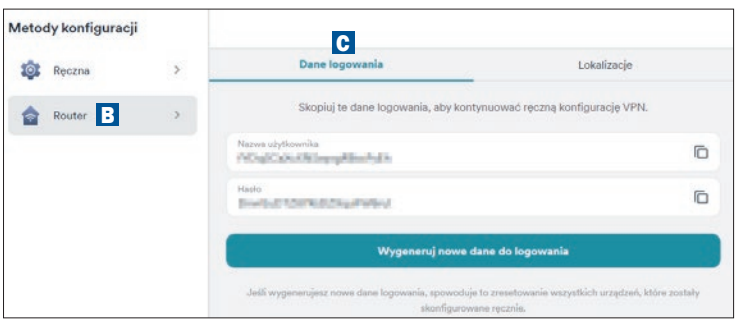
SURFSHARK NA DOWOLNYM URZĄDZENIU W SIECI DOMOWEJ

Po zakończeniu konfigurowania usługi VPN na smartfonie lub komputerze możemy również skonfigurować w odpowiedni sposób router lub punkt dostępowy w systemie Windows, dzięki czemu urządzenia w naszej sieci, na przykład konsola, telewizor czy Chrome cast, będą również mogły skorzystać z zalet i możliwości usługi VPN. W wypadku niektórych routerów możliwe jest takie ich skonfigurowanie, by cały ruch naszej sieci domowej był transferowany przez VPN. Urządzenia takie należą jednak do rzadkości, a konfiguracja nie jest najprostsza. Dysponując routerem, który dostarczają operatorzy internetu czy telewizji kablowej, praktycznie można zapomnieć o takiej możliwości. Jeśli jednak mamy odpowiednie urządzenie, nic nie stoi na przeszkodzie, by cały ruch sieci domowej kierować przez VPN. Alternatywnie możemy w Windows 10 uruchomić dedykowany punkt dostępowy – zamiast z routerem nasze urządzenia połączymy z nim, by zabezpieczyć transmisję VPN-em. Drugie rozwiązanie jest ostatecznością, gdyż z uwagi na ograniczenia kart Wi-Fi w komputerach i laptopach na pewno doświadczymy spadków prędkości połączeń: tego nie da się przeskoczyć.

KONFIGURUJEMY ROUTER

Bezpośrednio do łączenia z VPN-em możemy wykorzystać routery używające oprogramowania: DD-WRT, AsusWRT, Tomato lub OpenWRT. Najłatwiej zrobimy to, wykonując po kolei punkty porad umieszczonych na stronie Surfsharka. Do nawiązania połączenia będziemy jednak potrzebowali danych logowania (innych niż nasz login i hasło do Surfsharka) oraz adresu serwera VPN, z którym nawiążemy połączenie.



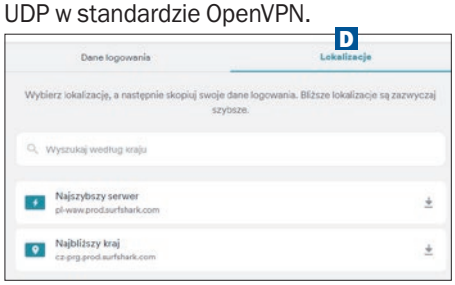


1 Otwieramy stronę **my.surfshark.com/vpn/manual-setup/main**. W lewej części okna klikamy na **Konfiguracja ręczna** A, a po prawej na **Router** B.

2 Nazwę użytkownika oraz hasło logowania znajdziemy po kliknięciu na **Dane logowania** C. Zapisujemy widoczne dane najlepiej w pliku tekstowym, skąd łatwo będzie nam je ponownie skopiować.

3 Adres serwera kopiujemy z zakładki **Lokalizacje** D. Zapisujemy widoczne dane

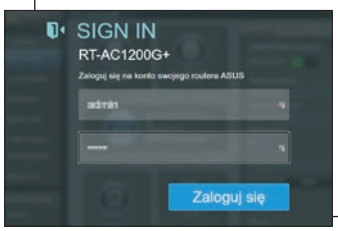
– po uprzednim wybraniu lokalizacji serwera VPN. Możemy również pobrać pliki z gotowymi konfiguracjami dla protokołów TCP oraz UDP w standardzie OpenVPN.



4 Aby dotrzeć do poradników konfiguracyjnych routerów, klikamy na **Konfiguracja ręczna**, potem na **Router** i w prawej części w sekcji **Samouczki** na nazwę oprogramowania używanego przez nasz router.

Konfiguracja routera Asusa z obsługą OpenVPN

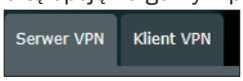
Poznajmy przykładową procedurę krok po kroku na bazie routera **Asusa**, który wspiera obsługę protokołu OpenVPN:



1 Logujemy się do panelu administratorskiego na naszym routerze.

2 Następnie po lewej stronie klikamy na **VPN** E.

3 Przechodzimy do zakładki **Klient VPN**, klikając na tę opcję na górnym pasku.



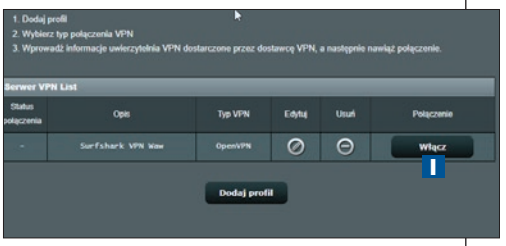
4 Teraz u dołu okna klikamy na **Dodaj profil** F.

5 Następnie klikamy na **OpenVPN**, podajemy dowolny opis, w polu **Nazwa użytkownika** podajemy dane skopiowane z naszego konta Surfshark, podobnie w polu **Hasło**.

6 Klikamy na **Wybierz plik** G i wskazujemy pobrany wcześniej plik konfiguracyjny z rozszerzeniem **.ovpn** w protokole UDP dla wybranego serwera i klikamy na **Uploaduj**.

7 Po pojawieniu się informacji **Zakończono** H klikamy na **OK**. **Uwaga!** Nie zaznaczamy opcji importowania pliku CA.

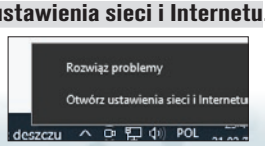
8 Teraz pozostaje nam jedynie kliknąć na **Włącz** I przy dodanym profilu. Dzięki temu nasz router połączy się z serwerem Surf shark i nawiąże połączenie z wybranym serwerem. Cały ruch sieciowy, który będzie przechodzić przez nasz router, będzie przechodził przez VPN. To rozwiązanie pozwala więc, aby wszystkie urządzenia w naszej sieci były bezpieczne. Jeśli chcemy przełączać się pomiędzy różnymi serwerami, musimy dodać profile do każdego z nich osobno.



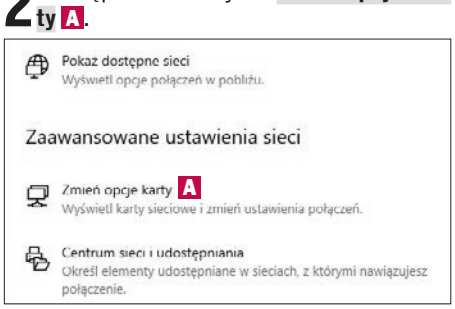
TWORZYMY PUNKT DOSTĘPOWY W WINDOWS

Jeśli nie dysponujemy odpowiednim sprzętem, możemy skonfigurować komputer z systemem Windows tak, aby pełnił rolę routera VPN, przez który inne urządzenia będą nawiązywać połączenie. Ta metoda zadziała w wypadku każdego urządzenia, które podłączymy do utworzonego punktu dostępowego – smart TV, konsoli, Chromecasta. Niestety, wiąże się to z dość sporym spadkiem wydajności względem korzystania z routera. **Uwaga!** Komputer musi mieć bezprzewodową kartę sieciową, aby było możliwe wykonanie opisanych kroków.

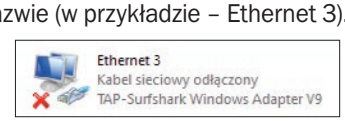
1 Prawym przyciskiem myszy klikamy na ikonę połączenia kablowego lub Wi-Fi w zasobniku systemowym i wybieramy **Otwórz ustawienia sieci i Internetu**.



2 Następnie klikamy na **Zmień opcje karty** A.

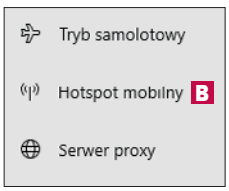


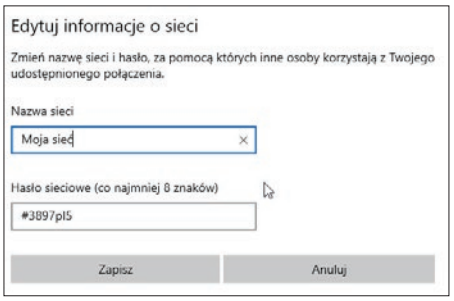
3 W nowym oknie odszukujemy i zapamiętujemy nazwę połączenia z **TAP-Surfshark** w nazwie (w przykładzie – Ethernet 3).



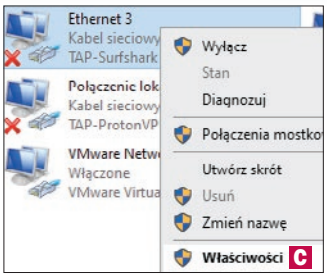
4 W otwartym wcześniej oknie ustawień sieci i internetu klikamy na **Hotspot mobilny** B.

5 Klikamy na **Edytuj**, ustawiamy nazwę sieci zabezpieczonej przez VPN oraz hasło.



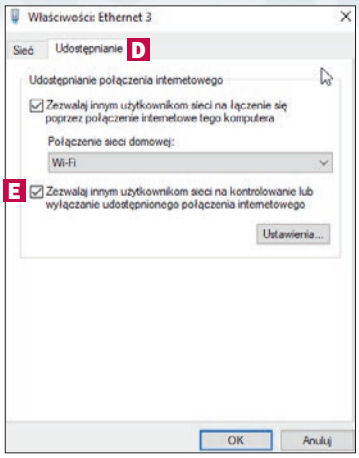


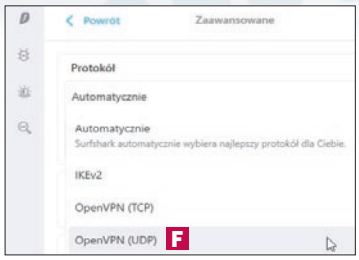
6 Potem u góry okna przesuwamy przełącznik na pozycję **Włączone**. W oknie z punktu **1** pojawi się nowe połączenie z oznaczeniem **Microsoft Wi-Fi Direct**.



7 W oknie z punktu **1** klikamy prawym przyciskiem myszy na połączenie **TAP-Surfshark** i wybieramy **Właściwości C**.

8 Przechodzimy na zakładkę **Udostępnianie D**. Zaznaczamy opcję **Zezwalaj innym użytkownikom... E**, a potem wybieramy z aktywnej listy połączenie, które pojawiło się po wykonaniu poprzedniego kroku. Klikamy na **OK**.





9 Teraz w aplikacji Surfshark klikamy na **Ustawienia**, **Zaawansowane**. W sekcji **Protokół** wybieramy **OpenVPN (UDP) F**. Następnie łączymy się z siecią VPN na komputerze.

10 Teraz wystarczy, abyśmy połączyli się z naszym nowo utworzonym punktem dostępu na urządzeniu, na którym chcemy korzystać z usługi VPN (telewizor, konsola itp.).

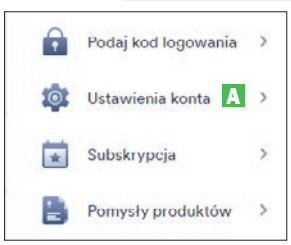
DODATKOWE ŚRODKI BEZPIECZEŃSTWA

Usługa SurfShark VPN to nie tylko rozwiązanie pozwalające na anonimowe surfowanie po sieci, ale też sposób na monitorowanie, czy nasze dane nie padły łupem hakerów w wyniku ataku na jakiś serwis internetowy, w którym mamy konto. Dostęp do dodatkowych funkcji w usłudze Surfshark, czyli monitorowania wycieków danych, takich jak e-mail czy dane kart płatniczych, wymaga aktywacji dodatkowego pakietu **Alert** w samej usłudze. Jest on płatny niecałe 6 złotych miesięcznie. Oprócz wniesienia opłaty trzeba jeszcze podnieść poziom bezpieczeństwa korzystania z usługi Surfshark VPN poprzez aktywację uwierzytelniania dwuskładnikowego. Wszelkie operacje przeprowadzamy za pomocą przeglądarkowego interfejsu usługi dostępnego za pośrednictwem adresu **my.surfshark.com**.

UWIERZYTELNIANIE DWUSKŁADNIKOWE NA SMARTFONIE

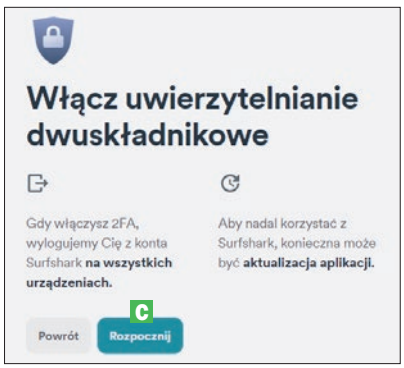
Po wykupieniu dodatkowego pakietu usługi **Alert** i zatwierdzeniu jej warunków w oknie przeglądarki zostaniemy poinformowani, że musimy włączyć uwierzytelnianie dwuskładnikowe. Warto to zrobić, nawet jeśli nie planujemy aktywować tej usługi. Uwierzytelnianie dwuskładnikowe znacznie zwiększa nasze bezpieczeństwo – warto więc z niego korzystać i to nie tylko w przypadku Surfshark VPN.

1 W aplikacji Surfshark VPN naciskamy w prawym górnym rogu ikonę naszego konta, a następnie **Ustawienia konta A**.

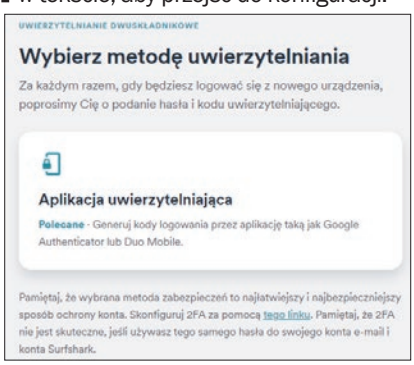


2 Teraz po prawej stronie w sekcji **Uwierzytelnianie dwuskładnikowe** naciskamy **Włącz 2FA B**.

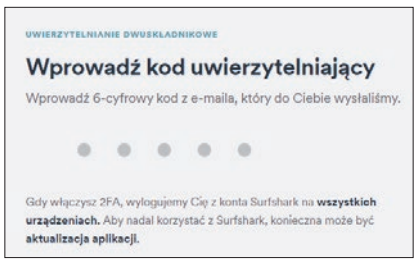
3 Na kolejnej stronie naciskamy **Rozpocznij C**.



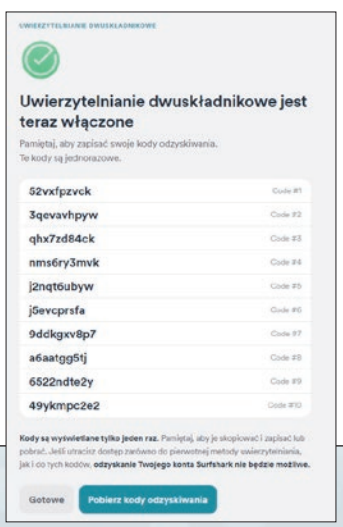
4 Naciskamy podświetlony na niebiesko link w tekście, aby przejść do konfiguracji.



5 Po chwili zostanie do nas wysłany e-mail z kodem uwierzytelniającym, który musimy podać na kolejnym ekranie. Po podaniu kodu naciskamy **Dalej**.



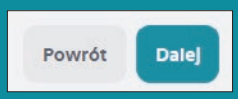
6 Na koniec należy pobrać lub zapisać jednorazowe kody odzyskiwania. Jeśli utracimy dostęp do pierwotnej metody uwierzytelniania i dodatkowo zgubimy kody, nie będziemy w stanie odzyskać dostępu do konta Surfshark.



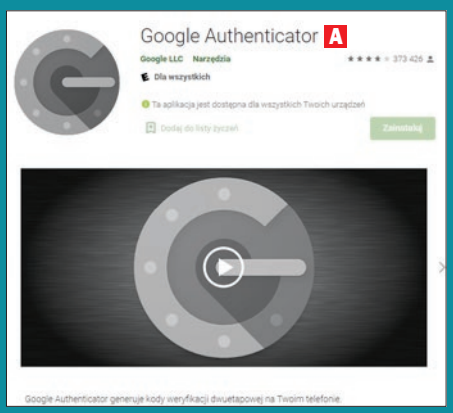
UWIERZYTELNIANIE PRZEZ APLIKACJĘ MOBILNĄ

Zdecydowana większość użytkowników korzysta ze znacznie prostszej metody dodatkowej autentykacji, wykorzystując specjalne aplikacje na smartfonie, na przykład Google Authenticator. Zobaczmy, jak skonfigurować autoryzację przez tę mobilną aplikację – znacznie ułatwi to uwierzytelnianie dwuskładnikowe.

1 Wykonujemy pierwsze trzy kroki z poprzedniej porady, potem jednak nie naciskamy linku, ale **Dalej** u dołu okna.

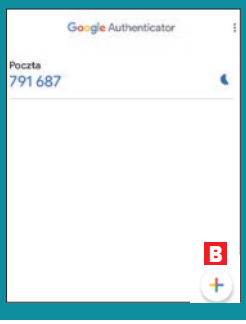


2 Na ekranie pojawi się kod QR, który musimy zeskanować w aplikacji uwierzytelniającej.

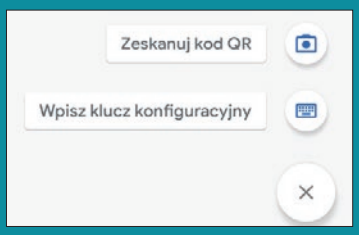


3 Instalujemy ze sklepu aplikację **Google Authenticator A**.

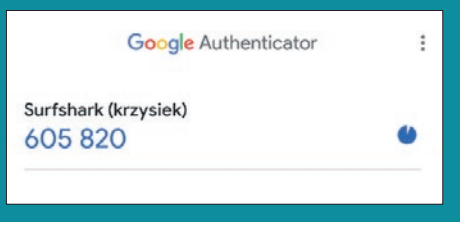
4 Po uruchomieniu aplikacji dotykamy w dolnym prawym rogu plusa **B** w celu dodania nowego konta.



5 Następnie wybieramy opcję **Zeskanuj kod QR** i skanujemy kod lub wpisujemy klucz, korzystając z opcji **Wpisz klucz konfiguracyjny**.



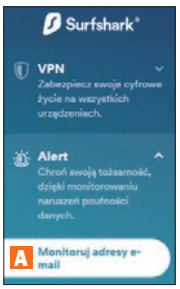
6 Po chwili kody autoryzacyjne będą generowane dla naszego konta i zawsze, gdy będziemy chcieli się zalogować, będziemy musieli mieć przy sobie telefon i skorzystać z generowanych automatycznie kodów autoryzacyjnych.



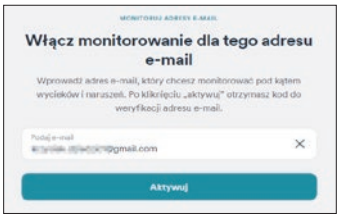
MONITOROWANIE ADRESU E-MAIL

Jedną z funkcji, do jakich uzyskamy dostęp po aktywowaniu pakietu **Alert**, jest monitorowanie adresów e-mail. Wystarczy podać swój adres, a będzie on monitorowany pod kątem wycieków i naruszeń. Dzięki temu dowiemy się, jeśli nasz adres stanie się publicznie dostępny.

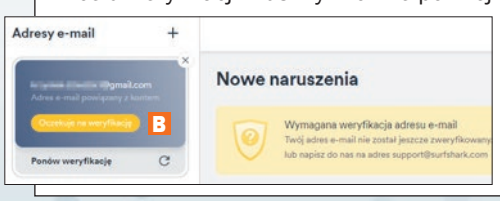
1 Na stronie o adresie **my.surfshark.com** po lewej stronie klikamy na **Alert**, a następnie na **Monitoruj adresy e-mail A**.



2 Następnie wprowadzamy nasz adres e-mail i klikamy na **Aktywuj**.

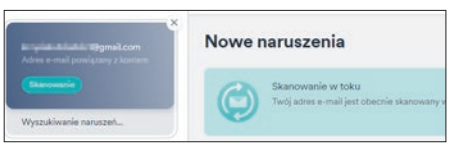


3 Po chwili status naszego adresu zostanie zmieniony na **Oczekuje na weryfikację B**. W celu weryfikacji musimy w oknie poniżej podać kod, który zostanie wysłany na nasz adres e-mail.

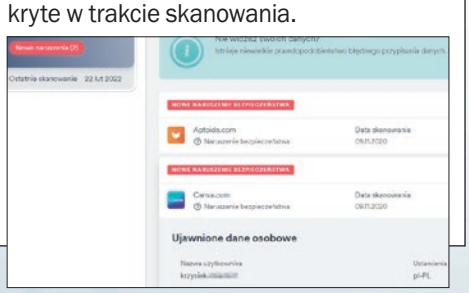


4 Wprowadzamy kod weryfikacyjny i klikamy na **Zweryfikuj adres e-mail**.

5 Po chwili nasz adres zostanie zweryfikowany i rozpocznie się skanowanie. Może ono potrwać około dwóch minut.



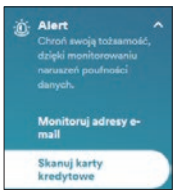
6 W naszym przykładzie zostały wykryte dwa naruszenia bezpieczeństwa, które miały miejsce jakiś czas temu. Dane uzyskane przez skaner, do których mają dostęp hakerzy i nie tylko, w przykładzie niestety są poprawne. Zaleca się w takim przypadku zmianę hasła do kont, które zostały wykryte w trakcie skanowania.



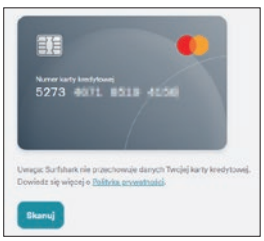
NARUSZENIA KART

Ciekawą funkcją modułu **Alert** jest możliwość skanowania karty kredytowej. Działa to na tej samej zasadzie co monitorowanie adresu e-mail.

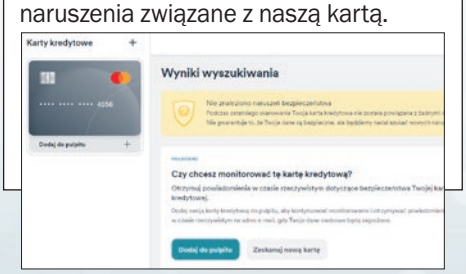
1 Na stronie o adresie **my.surfshark.com** po lewej stronie klikamy na **Alert**, a następnie na **Skanuj karty kredytowe**.



2 Następnie wprowadzamy nasz numer karty i klikamy na **Skanuj**.



3 Od razu zostaniemy poinformowani o ewentualnych znalezionych naruszeniach. Możemy dodać wiele kart, wystarczy klikać na **Zeskanuj nową kartę**. Możemy również dodać naszą kartę do pulpitu, dzięki czemu od razu po zalogowaniu będziemy wiedzieli, czy pojawiły się jakieś nowe naruszenia związane z naszą kartą.



DODATKOWE FUNKCJE SURFSHARKA

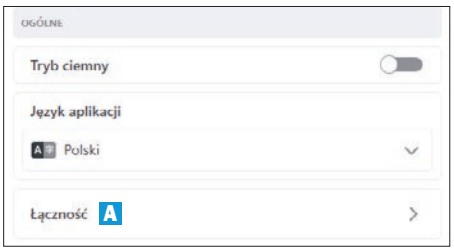
Oprócz podstawowych działań, jak nawiązywanie połączenia z wybranym serwerem i wybieranie konkretnych serwerów, Surfshark oferuje wiele zaawansowanych funkcji, których nie znajdziemy u konkurencji. Warto wiedzieć, gdzie one się znajdują, jak z nich korzystać i do czego mogą się nam przydać.

SURFSHARK BYPASSER

Funkcja **Bypasser** była już wspomniana na stronie 6. Służy ona do kierowania części ruchu sieciowego na naszym komputerze poprzez VPN, a części bez takiej ochrony. Niektóre aplikacje wymagają od nas tego, aby połączenie nie było kierowane przez VPN. Możemy zrobić dla nich odpowiedni wyjątek, a pozostały ruch sieciowy nadal będzie chroniony.

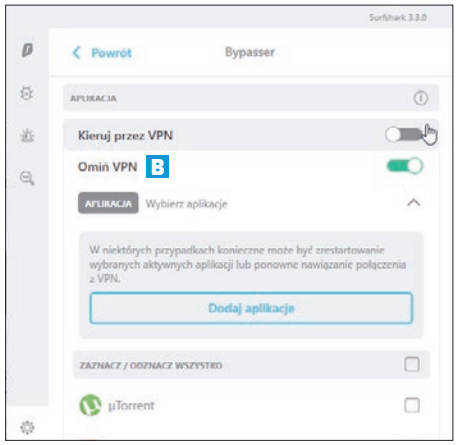
1 W celu aktywowania tej funkcji uruchamiamy aplikację **Surfshark VPN**, logujemy się na nasze konto i klikamy w dolnym lewym rogu na **Ustawienia**.

2 Następnie klikamy na **Łączność** A w kategorii **Ogólne**.



3 W kolejnym oknie klikamy na **Bypasser**.

4 Klikamy na **Omiń VPN** B, rozwijamy listę aplikacji i zaznaczamy te, których ruch sieciowy ma nie być kierowany przez VPN.



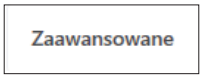
5 Możemy również zdefiniować konkretne strony internetowe, aby zawsze były wykluczane z ruchu VPN.

IP ROTATOR

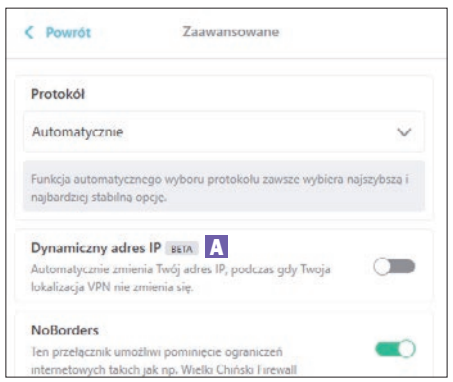
IP Rotator to pierwsza z funkcji dostępnych w ramach pakietu Nexus. **Dynamiczny adres IP** – pod taką nazwą znajdziemy tę funkcję w ustawieniach – umożliwia automatyczną zmianę naszego adresu IP bez rozłączania nas z usługą VPN.

1 W celu aktywowania tej funkcji uruchamiamy aplikację **Surfshark VPN**, logujemy się na nasze konto i klikamy w dolnym lewym rogu na **Ustawienia**.

2 Następnie klikamy na **Zaawansowane** w kategorii **Ogólne**.



3 Teraz należy aktywować funkcję **Dynamiczny adres IP** A.



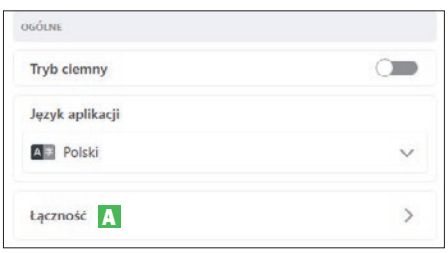
4 Na koniec klikamy na **Rozumiem** B po zapoznaniu się z metodą działania tej funkcji.

CLEANWEB

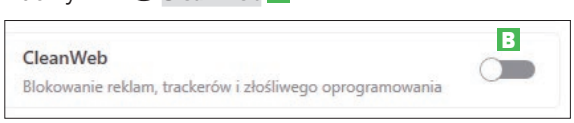
Funkcja **CleanWeb** pozwala w trakcie korzystania z usługi VPN blokować reklamy, trackery i złośliwe oprogramowanie.

1 W celu aktywowania tej funkcji uruchamiamy aplikację **Surfshark VPN**, logujemy się na nasze konto i klikamy w dolnym lewym rogu na **Ustawienia**.

2 Następnie klikamy na **Łączność** A w kategorii **Ogólne**.



3 W kolejnym oknie aktywujemy usługę **CleanWeb** B.



SKĄD WZIĄĆ PROGRAM SURFSHARK VPN

Surfshark VPN możemy kupić na stronie o adresie **order.surfshark.com**.

Są dostępne trzy plany:

- miesięczny (płacimy co miesiąc 53,54 złotego),
- 12-miesięczny (płacimy rocznie 237,78 złotego),
- 24-miesięczny (płacimy 247,06 złotego za 24 miesiące, a po ich upływie – rocznie; tego planu dotyczy 83-procentowy rabat dla Czytelników z kodem PL2022).

USUWANIE TREŚCI Z INTERNETU

Czasem w internecie dochodzi do wycieku danych. Ktoś może opublikować nasze zdjęcia bez naszej zgody, napisać obraźliwe i nieprawdziwe informacje na nasz temat lub upublicznić jakieś prywatne informacje, które nie powinny znaleźć się w sieci.

Na szczęście możemy starać się usuwać takie treści. Należy jednak pamiętać, aby postępować zgodnie z pewnym ustalonym porządkiem.

Przede wszystkim należy zwrócić się do administratora danej strony z prośbą o usunięcie konkretnej treści, podając swoje argumenty. Możemy dochodzić swoich praw w sądzie, gdyby administrator odmówił usunięcia treści.

Następnie musimy zwrócić się z prośbą do administratorów popularnych wyszukiwarek. Najczęściej prośby o usunięcie z wyników wyszukiwania trafiają do Google, gdyż nawet jeśli administrator usunie obraźliwe informacje na nasz temat, mogą być one nadal wyszukiwane w Google, ponieważ serwis indeksuje i zapisuje witryny na swoich serwerach.

WAŻNE

Wyszukiwarka Google pokazuje informacje ze stron internetowych. Nawet jeśli usuniemy wskazane treści z wyszukiwarki Google, mogą one wciąż być dostępne w internecie. Oznacza to, że nadal będzie można zobaczyć je na stronie, na której zostały zamieszczone, oraz w mediach społecznościowych, i znaleźć przez inne niż Google wyszukiwarki. Niezbędny może być kontakt z webmasterem witryny i poproszenie go o usunięcie materiałów. Jeśli nie jesteśmy w stanie doprowadzić do usunięcia treści przez właściciela strony, Google może usunąć dane osobowe, w przypadku których istnieje duże ryzyko, że zostaną wykorzystane do kradzieży tożsamości albo dokonania nadużyć finansowych lub innych szkód.

ZGŁASZANIE USUWANIA TREŚCI Z WYBRANYMI INFORMACJAMI PRYWATNYMI PRZEZ GOOGLE

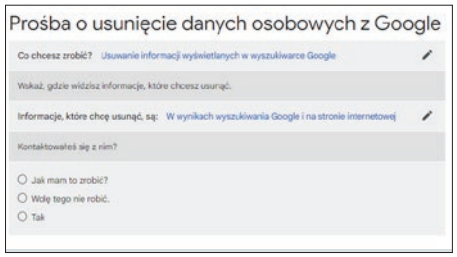
Przeczytajmy, w jaki sposób złożyć prośbę o usunięcie z wyszukiwarki Google prywatnych danych. Według informacji dostępnej na stronie Google, zostanie rozpatrzone usunięcie treści, które zawierają:

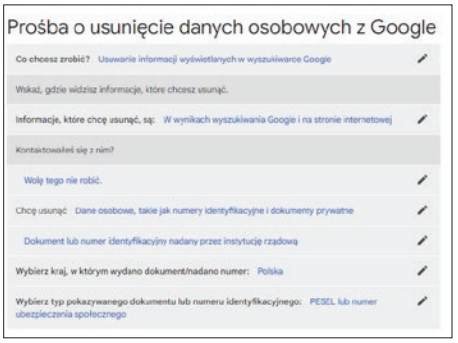
- poufne krajowe numery identyfikacyjne – na przykład PESEL;
- numer konta bankowego;
- numer karty kredytowej;
- zdjęcia podpisu;
- poufna dokumentacja medyczna.

1 Wchodzimy na stronę **https://support.google.com/websearch/troubleshooter/9685456#ts=2889054%2C2889099**

2 Następnie wybieramy opcję **Wolę tego nie robić**, **Dane osobowe…**, **Dokument lub numer…**, jako kraj wskazujemy **Polskę** i typ dokumentu **PESEL**.

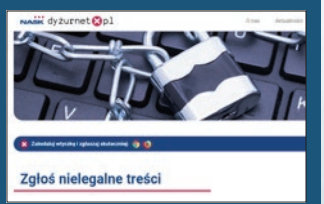
3 Po podaniu tych danych pojawi się rozbudowany formularz, który musimy wypełnić. Musimy w nim między innymi podać treści, które chcemy usunąć, i wskazać adresy internetowe, na których znajdują się treści do usunięcia. Dodatkowo warto załączyć zrzuty ekranu, aby osoba, która będzie weryfikować zgłoszenie, mogła szybko odnaleźć treści, o które nam chodzi. Warto również uzasadnić swoje zgłoszenie. By wysłać formularz, klikamy u dołu strony na **Wyślij**.





NIELEGALNE I SZKODLIWE TREŚCI W INTERNECIE

Jeśli natrafimy w internecie na nielegalne treści, czyli takie, które naruszają przepisy polskiego prawa, powinniśmy udać się na stronę: **dyzurnet.pl/zglos-nielegalne-tresci** i dokonać zgłoszenia. W przypadku zniesławień możemy zebrać materiał dowodowy i zgłosić się z nim do odpowiednich służb – do policji lub prokuratury.



WARTO WIEDZIEĆ

Warto wiedzieć, że Google otrzymuje zgłoszenia od mieszkańców państw na całym świecie z prośbami o usunięcie treści. Co ciekawe, krajem, z którego w ciągu ostatnich 10 lat było najwięcej zgłoszeń, jest Rosja z wynikiem 123 606 zgłoszeń. Na drugim miejscu znalazła się Turcja – 14 231 zgłoszeń. Polska natomiast jest na 27. miejscu z zaledwie 235 zgłoszeniami na przestrzeni ostatnich 10 lat.

Większość państw jako główną przyczynę usunięcia treści z Google podaje „Zniesławienie".

	KRAJ	GŁÓWNY POWÓD	ZGŁOSZENIA DLA TEGO POWODU	ŁĄCZNA LICZBA ZGŁOSZEŃ
1	Rosja	Bezpieczeństwo narodowe	41 502	123 606
2	Turcja	Zniesławienie	5543	14 231
3	Indie	Zniesławienie	2757	9899
4	Stany Zjednoczone	Zniesławienie	5793	9627
5	Brazylia	Zniesławienie	3757	8148
6	Korea Południowa	Inne	2349	5330
7	Wielka Brytania	Bezpieczeństwo narodowe	1574	4387
8	Francja	Bezpieczeństwo narodowe	1493	4231
9	Niemcy	Zniesławienie	1978	3925
10	Włochy	Zniesławienie	1179	2112

Komputer Świat od 1998 roku

Adres redakcji: 02-672 Warszawa, ul. Domaniewska 49
internet: www.komputerswiat.pl, forum.komputerswiat.pl
e-mail: redakcja@komputerswiat.pl

Krzysztof Dziedzic: autor tekstów

Rafał Kamiński: redaktor naczelny

Tomasz Paczuski: z-ca redaktora naczelnego, szef wydania drukowanego

Agnieszka Al-Jawahiri: z-ca redaktora naczelnego, szef wydań specjalnych

Jolanta Rososińska: korekta
Robert Dobrzyński: dyrektor artystyczny
Mariusz Rybak: redaktor graficzny

ringier axel springer

Wydawca: RINGIER AXEL SPRINGER POLSKA Sp. z o.o.
Członek Izby Wydawców Prasy i Związku Kontroli Dystrybucji Prasy
www.ringieraxelspringer.pl, asp@axelspringer.pl
Adres: 02-672 Warszawa, ul. Domaniewska 49
tel. (12) 2600200 (BOK)

Prezes Zarządu: Mark Dekan
Prezes Honorowy: Wiesław Podkański
Dyrektor Generalny: Marcin Biegluk
Dyrektor Finansowy: Krzysztof Stopa
Dyrektor Sprzedaży: Mariusz Wąsiński
Dyrektor Marketingu: Olga Korolec

media impact

Biuro reklamy: Media Impact
reklama.warszawa@mediaimpact.pl
tel. (12) 2600200 (BOK)

Business Project Manager: Paweł Bulwan
Dział personalny: Monika Remiszewska
Księgowość: Katarzyna Fita (dyrektor)
Kolportaż: Rafał Kamiński (dyrektor)
Produkcja: Mariusz Gajda
Druk: Walstead Kraków Sp. z o.o.

Prenumerata i egzemplarze archiwalne:
www.literia.pl

Sprzedaż internetowa: www.literia.pl
Prenumerata zagraniczna: www.literia.pl
E-wydania: ksplus.pl

Redakcja nie zwraca materiałów niezamówionych, zastrzega sobie prawo redagowania nadesłanych tekstów, nie odpowiada za treść zamieszczanych reklam i ogłoszeń

Zabroniona jest bezumowna sprzedaż czasopisma po cenie niższej od ceny detalicznej ustalonej przez wydawcę. Sprzedaż numerów aktualnych i archiwalnych po innej cenie jest nielegalna i grozi odpowiedzialnością karną.